

# POLYPHASE AND FREQUENCY HOPPING SEQUENCES OBTAINED FROM FINITE RINGS

*A Thesis Submitted  
in Partial Fulfilment of the Requirements  
for the Award of the Degree of*

**DOCTOR OF PHILOSOPHY**

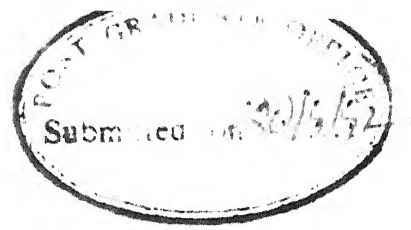
*by*

UDAYA P

*to the*

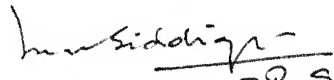
DEPARTMENT OF ELECTRICAL ENGINEERING  
INDIAN INSTITUTE OF TECHNOLOGY KANPUR

*September 1992*



## CERTIFICATE

It is certified that the work contained in the thesis entitled POLYPHASE AND FREQUENCY HOPPING SEQUENCES OBTAINED FROM FINITE RINGS by *Udaya P* has been carried out under my supervision and that this work has not been submitted elsewhere for the award of a degree.

  
M U SIDDIQI 28.9.92

Professor

Department of Electrical Engineering  
Indian Institute of Technology Kanpur

September 1992.

POST GRADUATE DEPARTMENT

EE-1882-D-UDA-POL

19 OCT 1993/EE

CENTRAL LIBRARY  
111 KANPUR

Acc. No. A.116564

To My Parents and

द्वा सुपर्णा सयुजा सखाया  
समानं वृक्षं परिषस्वजाते  
तयोरन्यः पिप्पलं स्वाद्वत्त्य  
नश्नन्नन्यो अभिचाकशीति

संस्कृत ११.१.१६४.२०

"Two birds, closely bound companions—  
clasp close one and the same tree.  
Of these two, the one eats the sweet berry,  
the other, not eating, only looks on."

Rig Veda I.164.20



# ACKNOWLEDGEMENTS

In my very useful and memorable five and half year stay at I.I.T, Kanpur, I have come across many noble souls who have broadened my vision in academics as well as in the outlook of life, and they have immensely helped towards my overall development and conduct. To all of them I express my deepest sense of gratitude. I am highly indebted to this institute for having provided a free academic environment to learn whatever I wished.

Dr M.U. Siddiqi as my teacher and thesis supervisor has guided me throughout my studies in the institute. He was willing to help me in whatever difficulties I have faced. His many timely comments and advices have helped me to know my limitations and I am immensely benefited from them. This thesis owes a lot to his patient guidance, critical comments and suggestions at various stages of the work. He has gone through the entire thesis many times in his characteristic way, suggesting several structural changes which improved the overall presentation. No words of gratitude will ever suffice for his genuine concern for my growth.

I express my sincere gratitude to my teacher Dr. V.P. Sinha, for introducing me to algebraic ideas in Signal processing and for his constant encouragement throughout my studies here.

I express my heartfelt gratitude to Dr N.L. Arora for moulding my outlook and conduct. I have greatly benefited from his Yoga lessons.

I express my heartfelt thankfulness to my teachers Dr. R Sharan, Dr. P.R.K Rao, Dr. V Sinha, Dr. S.P Mohanty and Dr M.C. Bhandari for their inspiring lectures. I am grateful to each one of them for their constant encouragement and advice.

Dr. T.K Chandarshekar, Dr. M. Sachchidananda, Dr. S.S. Prabhu, Dr. T.G. Gangadharayya, Dr. Raghavendra, Mr. Muddappa, Mr. Narayan have provided me homely atmosphere and friendship. They were always very kind and helpful. I cannot adequately express my gratitude to them.

Madhusudhana has been my close friend and colleague for many years. We have learnt and discussed many things together. I have no words to express my thankfulness to him.

Venkatesh, Deepak, Aravind, Venu, Hari, Ganesh, have taken a lot of trouble in helping me in preparing this thesis. I am highly indebted to each one of them for their cooperation and helpfulness. I express my heartfelt thanks to them and many other friends who have made my stay at this place pleasant and memorable.

I am very happy to thank Mr. D.V.S.S.N Murthy for his help in taking printout of the thesis and Dr Sachchidanand for extending the printing facilities.

I express my appreciation to Messrs Chourasiya Xerox Center for excellent photocopying and Ahmed Book Center for neat binding of the thesis.

Finally, whatever little I have done I owe to my parents, brothers and sister. I have no words to express my thankfulness for their love and affection which has been my major source of strength.

# SYNOPSIS

Name of Student : Udaya P

Roll No : 8620462.

Degree for which submitted : Ph. D

Department : Electrical Engineering.

Thesis Title: Polyphase and Frequency Hopping Sequences  
obtained from Finite Rings

Name of the Supervisor: Dr. M. U. Siddiqi.

Month and Year of thesis submission : June, 1992.

This thesis is concerned with algebraic construction of sequences obtained from residue class finite rings and with their periodic correlation and linear complexity (LC) properties. Such sequences are of interest in polyphase and frequency hopping code division multiple access (CDMA) communication systems. The finite rings considered in this study are:

- Residue class integer ring modulo  $M$ :  $Z_M$
- Residue class polynomial ring  $GF(p)[\xi] \bmod w(\xi)$ :  $P_p^n[w(\xi)]$ , where  $w(\xi)$  is an  $n^{\text{th}}$  degree polynomial over  $GF(p)$ .

CDMA communication systems require a large set of sequences, in which each sequence is easily distinguished from every other sequence in the set and from all time shifted versions of itself. The criteria of distinguishability of sequences depends on the type of modulation and the type of channel. Some times, security considerations demand the sequences to be random and to possess large LC [1]. For the construction of required sequences, a wide range of properties which affect the system performance have been considered in literature [2]. Since the requirements on sequences differ from problem to problem, approaches to sequences construction are specific to the problem.

The sequences in this thesis are viewed as polynomial mappings of trace functions of unit elements of Galois extension rings. The periodic correlation properties (correlation values and their distribution) of sequences over  $Z_4$  are obtained by using an abelian association scheme on the elements of the Galois extension ring of  $Z_4$ . For sequences over residue class polynomial rings, the correlation properties have been obtained by utilizing the vector space structure of the polynomial ring and the properties of finite field  $m$ -sequences. The LC of sequences has been computed by using a finite ring version of Blahut's complexity theorem for finite field case..

The approach used to obtain the desired sequences is shown in Fig 1. It may be called structural approach. In this approach, sequences are constructed over a finite alphabet by using a sequence generation mechanism. Sequences over the finite alphabet are then transformed into real (complex) valued signals by an appropriate mapping  $\phi$ . A familiar example of such an approach is the generation of pseudo-noise sequences using feedback shift registers [3]; such sequences have a wide range of applications and there exists a large body of literature dealing with their various aspects.

The sequence generation mechanism is the core of the structural approach. It is dependent on the structure of the alphabet, and is independent of applications. Suitability of generated sequences for any specific application mainly depends on their properties. Hence major effort is required to determine their properties. Properties like period, linear complexity, and randomness ( $r$ -tuple distribution, run-length distribution), can be evaluated in the alphabet domain itself; such properties are called primary properties due to their direct dependence on the structure of the alphabet. However, evaluation of correlation properties depends on a mapping  $\phi$  from the alphabet to a subset of the real or complex-valued space; they are termed as secondary properties. The primary properties are better controlled because of their direct dependence on the sequence generation mechanism. However, the same is not true with the secondary properties, although they are more critical in practice. Note that in the structural approach the sequence design problem is not formulated by stating the constraints on the correlation parameters, it is sheer luck that some of the resulting sequences have nice properties to make them useful in practice.

Generalization of sequence alphabet from finite fields to finite rings yields lot of flexibility in choosing primary properties. Moreover, because of its specific properties, a finite ring structure is more suited to some communication systems. When a finite field is considered as the alphabet for sequence construction, the size of the alphabet is restricted to a prime or power of a prime number. Some

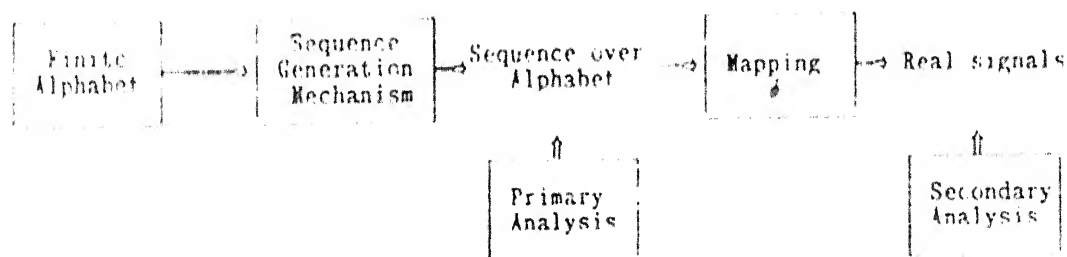


Fig 1: Structural Approach for Construction of Sequences

communication systems, like M-PSK modulated systems, demand alphabets of size other than a prime or a prime power. In such situations, a finite ring structure can provide a suitable alphabet. Also, in some modulation schemes which involve alphabets of size greater than two, finite rings can offer a much wider choice of alphabet size compared to finite fields. The period  $L$  of most of the algebraic sequences generated over finite fields is such that  $L$  divides  $V^r - 1$ , where  $V$  is the field cardinality and  $r$  is the degree of Galois field extension. This is because of the fact that the nonzero elements (units) of the  $r^{\text{th}}$  degree Galois extension of field  $\text{GF}(V^r)$  constitute a cyclic group of order  $V^r - 1$ ; the multiplicative order of elements in Galois extension field determines the period. In this respect, finite rings offer more flexibility, since the group of units of a Galois extension ring is in general abelian. For example, for sequences over  $Z_4$ , we can have periods  $2^r - 1$  and  $2(2^r - 1)$ .

Apart from the advantages cited above, residue class rings are also naturally suited for multiplexing operation. Decomposition of rings into internal direct sum of ideals, and the fact that the elements belonging to different ideals annihilate each other, play an important role in such applications [6].

To take care of various correlation functions of practical importance, a generalized correlation function between a pair of sequences is defined in the thesis such that the specific correlation functions can be derived from it as special cases. The definition of periodic correlation is assumed throughout the thesis.

Let  $A = \{a_0, a_1, \dots, a_{L-1}\}$ ,  $B = \{b_0, b_1, \dots, b_{L-1}\}$  be two sequences of period  $L$  over certain alphabet  $Q$  of size  $|Q|$ . Then the cross correlation function  $C_{AB}(\tau)$  between  $A$  and  $B$  is given by

$$C_{AB}(\tau) = \sum_{i=0}^{L-1} f\{\phi(a_i), \phi(b_{i+\tau})\}; \quad \tau = 0, 1, \dots, L-1 \quad (1)$$

where  $\phi$  is a mapping from the finite alphabet  $Q$  to an appropriate signal set which is a subset of real (complex) space, and  $f$  is a binary operation related to the definition of the correlation function which depends on the distance measure. The range of  $f$  is also a subset of real (complex) space. The nature of  $\phi$  and  $f$  depends on the type of modulation and the type of application where the sequences are used. The mapping  $\phi$  which links a finite ring and a signal set may be considered as an abstract modulator. Various correlation functions derived from Eq.(1) and considered in the thesis are binary, quaternary, and  $m$ -ary inner-product correlations, Hamming and Lee correlations, and block inner-product correlations (a generalized version of inner-product correlations).

For studying correlation properties of sequences, it is advantageous to define a correlation transform of sequences over finite rings. The correlation transform of a sequence  $A$  over a finite ring,

corresponding to a correlation function characterized by the 2-tuple  $(f, \phi)$ , is defined as the zeroth crosscorrelation between  $A$  and the all 0 sequence  $S^0$ , given by  $C_{AS^0}(0)$ .

Generalizations of the structure of alphabet give rise to flexibility in choosing primary properties; the same is not true with the secondary properties. Secondary properties have to be analyzed in each case for the suitability of sequences in specific applications. In an attempt to ease the secondary analysis, notion of a sequence alphabet matched to a signal set for a correlation function is proposed.

A finite ring  $\mathcal{R}$  is said to be matched to a signal set for correlation represented by a tuple  $(f, \phi)$  if and only if

$$f(\phi(a), \phi(b)) = f(\phi(a-b), \phi(0)); a, b \in \mathcal{R}, \quad (2)$$

where  $-$  is the subtraction in the finite ring  $\mathcal{R}$ . A simple example of a matched ring is that of a binary field  $GF(2)$  which is matched to biphase signal set for binary inner-product correlation. In this case, the additive group of  $GF(2)$  is isomorphically mapped to the multiplicative group of  $(1, -1)$  under the mapping  $\phi(a) = (-1)^a$ ;  $(1, -1)$  being the signal set for biphase signalling.

A detailed explanation of the motivation for taking up study of sequences over matched rings is as follows. Computation of correlation properties of sequences over matched rings is simplified by using combinatorial results concerning the correlation transform of sequences. The correlation operation of the signal set is isomorphic to addition in the alphabet structure and more importantly the mapping is linear. This allows us to make use of linearity of the ring alphabet for the computation of correlations. As a result, generalization of the alphabet structure from finite field to finite ring, in many situations, permits us to retain the advantages of linearity leading to simplicity in the analysis of sequences. Thus, while constructing sequences using the structural approach, it is advantageous to consider the matched ring structures. Further, sequences over matched structures may also have good properties. This belief is strengthened by the existence of optimal sets of quadriphase sequences obtained from  $\mathbb{Z}_4$  which is matched to quadriphase signal set for inner-product type correlation [4].

We have considered several examples of finite residue class rings matched to different signal sets for various correlations. Table 1 gives residue class rings matched to signal sets for various correlations. Several constructions of optimal signal sets derived from matched rings are given in the thesis.

The generalized correlation function defined by Eq.(1) depends on a pair of sequences. Some communication systems require correlation functions which depend on all the sequences employed in the system. We have considered such correlation functions, called generalized Hamming correlation functions. They are useful in slow frequency hopping spread spectrum systems, and are given as follows.

Let  $S^i$ ,  $m = 1, \dots, n$ , be  $n$  sequences of length  $L$  over certain alphabet  $Q$ , then the generalized Hamming crosscorrelation function concerning  $m^{\text{th}}$  sequence is given by

$$\text{GCH}_m(\tau_1, \tau_2, \dots, \tau_{m-1}, \tau_{m+1}, \dots, \tau_n) = \sum_{i=0}^{L-1} \text{gh}\{S^m_i; S^j_{i+\tau_j}, \text{ for all } j \neq m\}. \quad (3)$$

The corresponding autocorrelation function is given by

$$\text{GAH}_m(\tau_1, \tau_2, \dots, \tau_n) = \sum_{i=0}^{L-1} \text{gh}\{S^m_i; S^j_{i+\tau_j}, \text{ for all } j\} \quad (4)$$

where  $\text{gh}$  is a function given by

$$\begin{aligned} \text{gh}\{a; b_1, b_2, \dots, b_n\} &= 1 \text{ if } a \in \{b_1, b_2, \dots, b_n\} \\ &= 0 \text{ otherwise.} \end{aligned}$$

Equivalences of some correlation functions are also discussed in the thesis. Two correlation functions are equivalent if the computation of correlation values from one type is sufficient to determine the correlation values from the equivalent correlation function. Familiar examples of equivalent correlation functions are that of binary inner-product correlation and binary Hamming correlation. The equivalence of correlation functions is responsible for efficient digital implementation of some binary synchronization schemes based on Hamming correlation [5]. However, very few correlation functions with such a property exist. Extending the binary field results, binary block inner-product correlation is shown to be equivalent to binary block Hamming correlation.

## Main Results

Mainly local rings have been considered in the study since any general semi-local ring can be expressed as a direct sum of local rings. Properties of Galois extension rings of local finite residue class rings  $\mathbb{Z}_p^k$  and  $P_p^n[w^k]$ , where  $w^k$  denotes  $k^{\text{th}}$  power of an irreducible polynomial  $w(\xi)$  of degree  $m$  over  $\text{GF}(p)$  and  $n = mk$ , are used to generalize sequence generation procedures from their finite field counterparts. Galois extension rings here play a similar role as Galois extension fields in the case of finite fields. Two important Galois extension rings considered in the thesis are

- Galois extension ring of  $\mathbb{Z}_p^k$  of degree of extension  $r$ , denoted by  $\text{GR}(p^k, r)$ .
- Galois extension ring of  $P_p^n[w^k]$ , denoted by  $\text{PGR}(V^k, r)$ , where  $V$  represents the residue field  $P_p^m[w]$  of order  $p^m$  isomorphic to  $\text{GF}(p^m)$ .

Various families of sequences derived in the thesis are classified into the following classes.

- I. Families derived from local rings.
- II. Families derived from semi-local rings.

# I. Families derived from local rings:

## I(a) Linear Constructions

Here the sequences in a family are closed under pointwise ring addition. The familiar trace function representation of sequences over finite fields is generalized. Generalized automorphisms of Galois extension of residue class rings are employed to define a trace function from Galois extension ring to its ground ring. Then for any unit element  $\alpha$  which belongs to Galois extension ring, a family of sequences, called trace function sequences (or simply trace sequences) is defined. Since a local residue class ring contains a chain of local ideals, the family of trace sequences over a local ring also includes families of trace sequences over the ring ideals. The trace sequences over the proper ring are called zeroth level trace sequences and the trace sequences over ideals isomorphic to  $Z_p^\kappa$  or  $P_p^n[w^\kappa]$ ;  $1 \leq \kappa \leq k$ , are called  $(k-\kappa)^{th}$  level trace sequences. Thus altogether there are  $k$  level trace sequences.

The period of a trace sequence is determined by the multiplicative order of the unit element  $\alpha$  used to define the family, and hence, possible periods ( $L$ ) depend upon the structure of the group of units of the Galois extension ring. The group of units of a Galois extension ring is in general abelian which has a cyclic component group  $G_c$ , isomorphic to the group of units of its residue field. For example, the group of units of  $GR(4, r)$ ,  $GR^*(4, r)$  is of order  $2(2^r-1)$  with cyclic component group  $G_c$  of order  $2^r-1$ , which is isomorphic to group of units of  $GF(2^r)$ , the residue field of  $GR(4, r)$ . An unit element  $\alpha$  of the cyclic component group is called a primitive element if its multiplicative order is same as the order of the cyclic component group. The family of trace sequences is called a family of  $m$ -sequences or simply  $\mathcal{A}$  family if the unit element  $\alpha$  used to define the family is a primitive unit element of the Galois extension ring. The main difference between finite field and finite ring  $m$ -sequences is that there is only one cyclically distinct field  $m$ -sequence for a primitive element  $\alpha$  of  $GF(2^r)$ , whereas in the ring case there is a family of  $m$ -sequences corresponding to an element  $\alpha$  of the extension ring.

Three important families of sequences derived from  $\mathcal{A}$  families have been obtained. They are classified depending on their properties and the area of applicability.

1. Families of quadriphase sequences derived from  $\mathcal{A}$  families over  $Z_4$ .
2. Families of octa-phase sequences of period  $(2^r-1)$  from  $\mathcal{A}$  families over  $Z_8$ .
3. Families derived from  $\mathcal{A}$  families over the local ring  $P_p^n[w^k]$ .



*Families of quadriphase sequences derived from  $\mathcal{M}$  families over  $\mathbb{Z}_4^\#$* : Quadriphase sequences are constructed from sequences over  $\mathbb{Z}_4$  through a quadriphase mapping given by  $\phi(a) = \omega^a$ , where  $\omega = \sqrt{-1}$ . Two important families of quadriphase sequences derived from  $\mathcal{M}$  families over  $\mathbb{Z}_4$  are

(a) Families of quadriphase sequences of period  $(2^r-1)$ ; each family consisting of  $(2^r+1)$  sequences. The correlation transform distribution of these families is obtained by making use of the properties of an abelian association scheme defined over  $\text{GR}(4,r)$ . The crosscorrelation values belong to the set

$$\begin{aligned} \{(-1), (\pm 2^t - 1 \pm j 2^t)\} & \quad \text{for } r \text{ odd, } r = 2t + 1; j = \sqrt{-1} \\ \{(-1), (\pm 2^t - 1), (-1 \pm j 2^t)\} & \quad \text{for } r \text{ even } r = 2t, \end{aligned} \quad (5)$$

These families satisfy the Welch bound on  $\theta_{\max}$ . The number of cyclically equivalent families are shown to be equal to  $\phi(2^r-1)/r$ , where  $\phi$  is the Euler's  $\phi$  function which is equal to the number of integers  $\leq 2^r-1$  and relatively prime to  $2^r-1$ .

(b) Families of quadriphase sequences of period  $2(2^r-1)$ ; each family consisting of  $(2^{r-1}+1)$  sequences: Any group of units  $\text{GR}^*(4,r)$  of a Galois ring  $\text{GR}(4,r)$  is a direct product of two groups  $G_a$  and  $G_c$ , where  $G_a$  is Abelian group of order  $2^r$ , and  $G_c$  is the cyclic component group of order  $2^r-1$ . Associated with every element  $\gamma$  of  $G_a \in \text{GR}^*(4,r)$ ,  $\gamma \neq 1$ , a family of sequences of period  $2(2^r-1)$  is defined as a family of trace sequences generated by  $\gamma\alpha$ , where  $\alpha$  is a primitive element of  $G_c$ . Thus for every  $\alpha$ , there are  $2^r-1$  families. These sequences are shown to be interleaved  $m$ -sequences of period  $2^r-1$ , and hence are called interleaved  $m$ -sequence families, in short  $\mathcal{MK}$  families. The correlations are computed from the correlation values of  $m$ -sequences. Three classes of  $\mathcal{MK}$  families are identified depending on the nature of  $\gamma$ . They are

- (a)  $\mathcal{MK}^\gamma$  families with  $\text{trace}(\tilde{\gamma}) = 1$
- (b)  $\mathcal{MK}^\gamma$  families with  $\text{trace}(\tilde{\gamma}) = 0$ ,  $\gamma \neq 1$
- (c)  $\mathcal{MK}^3$  family

where  $\gamma = 1 + 2(\tilde{\gamma})$ ,  $\tilde{\gamma} = \gamma' \bmod 2$ ,  $\gamma' \in G_c$ . Out of the total  $2^r-1$  families,  $2^{r-1}$   $\mathcal{MK}^\gamma$  families with  $\text{trace}(\tilde{\gamma}) = 1$ , are optimal and satisfy Welch's bound on  $\theta_{\max}$ . Rest of the  $2^{r-1}-1$  families are suboptimal, wherein

# While preparing the thesis, we became aware of a paper by Boztas, Hammons, Kumar [7] which contains some of the results described here. This paper describes two families, Family A and Family B. These families correspond, as per our classification, to  $\mathcal{M}$  family and  $\mathcal{MK}^\gamma$  family with  $\text{tr}(\tilde{\gamma}) = 1$ . The  $\mathcal{MK}^\gamma$  families with  $\text{tr}(\tilde{\gamma}) = 0$  and the  $\mathcal{MK}^3$  family are additional sub-families among  $\mathcal{MK}$  families of period  $2(2^r-1)$ . The approach taken in this thesis for studying correlation properties of sequences is mainly based on the association schemes on  $\text{GR}(4,r)$  and the properties of  $\text{GR}(4,r)$ , whereas in [7], the theory of exponential sums is used for computing correlations. The framework used in the thesis takes care of all the results in [7] and appears to be more general than the one used in [7].

$\theta_{\max}$  is approximately equal to  $\sqrt{2L}$ ;  $L = 2(2^r - 1)$ . The  $\mathcal{JK}$  family is optimal only for the case when  $r$  is odd. The linear complexity of these sequences is equal to  $r$ , same as that of  $m$ -sequences.

*Families of octa-phase sequences of period  $(2^r - 1)$  from  $\mathcal{K}$  families over  $Z_8$ :* For any primitive element  $\alpha$ , family of  $m$ -sequences over  $Z_8$  consists of  $(4^r + 2^r + 1)$  sequences of period  $2^r - 1$ , which includes sequences over ideals  $\langle 2 \rangle$  and  $\langle 4 \rangle$ . Excluding the sequences over ideals  $\langle 2 \rangle$  and  $\langle 4 \rangle$ , there are  $4^r$  proper sequences over  $Z_8$ . These  $4^r$  proper sequences are divided into  $2^r$  sets each consisting of  $2^r$   $m$ -sequences which can be used for 8-PSK modulated CDMA communication systems. These sets satisfy what Massey has described as code sets satisfying Welch bound with equality [12] (Not Welch bound on  $\theta_{\max}$ ). This implies that  $\theta_{\text{rms}}$ , the root mean square of the inner product values between all pairs of various time shifted versions of sequences in a set  $F$  (expression for  $\theta_{\text{rms}}$  given below), is approximately equal to  $\sqrt{L}$ , and this is the smallest value possible.

$$\theta_{\text{rms}} = \frac{1}{M(ML-1)} \left( \sum_{\substack{X \in F \\ \text{except } X=Y}} \sum_{Y \in F} \sum_{\tau=0}^{L-1} |C_{XY}(\tau)|^2 \right),$$

where  $M, L$  are the size and period respectively of the sequences in the set. This is precisely the appropriate requirement for CDMA operations where many users are operating in the system.

*Families derived from  $\mathcal{K}$  sequences over the local ring  $P_p^n[w^k]$ :* Sequences over  $P_p^n[w^k]$  are used to derive frequency hopping patterns and sequences with good block inner-product correlations. Note that  $P_p^n[w^k]$  is a matched structure for both block inner-product and Hamming correlations. The frequency hopping patterns are obtained by associating with each symbol  $a$  in the ring  $P_p^n[w^k]$ , a distinct frequency  $f_a$  belonging to the frequency library. For efficient operation, it is required that mutual Hamming correlation between any two hopping patterns within a family should be small. A family of sequences over  $P_p^n[w^k]$ , denoted by  $\mathcal{K}(A)$ , is constructed, corresponding to each  $m$ -sequence  $S^A$ ,  $A \in \text{PGR}(V^k, r)$ . The number of sequences in  $\mathcal{K}(A)$  is determined by the number of distinct elements of  $P_p^n[w^k]$  occurring in  $S^A$ .

By making use of  $\mathcal{K}(A)$  families, where  $A \in \text{PGR}(V^k, r)$  and  $V$  is the order of the residue field,  $V^{r-\rho}$ ,  $0 \leq \rho \leq k$ , coincidence frequency patterns of size  $V^\rho$  and period  $V^r - 1$  are constructed. These frequency patterns meet Lempel and Greenberger bound on  $H_{\max}$  [1], which is the maximum of out of phase autocorrelation values and crosscorrelation values between any two hopping patterns. The derived frequency patterns include familiar one-coincidence frequency patterns.

Recently J.J. Komo and S.C. Liu [9] have described frequency hopping patterns from  $m$ -sequences over  $\text{GF}(2^r)$ . In [9], authors make note of a sequence over  $\text{GF}(2^2)$ , which is constructed by grouping two

binary  $m$ -sequences, sharing many properties of  $m$ -sequences and yet not an  $m$ -sequence over  $GF(2^2)$ . It is indeed an  $m$ -sequence over  $P_2^2[w^2]$  and rightly not an  $m$ -sequence over  $GF(2^2)$ . Our approach characterizes all such obtainable sequences by appropriately grouping  $m$ -sequences over finite fields. The weight distribution of  $m$ -sequences over  $P_p^n[w^k]$  is also given.

In addition to above results, we also derive a subset of  $m$ -sequences over  $P_p^n[w^k]$  having only two level block inner-product autocorrelation; out of phase auto correlation value being  $-n$ .

*I(b) Non-linear Constructions (Sequences with Controllable Linear Complexity):* The families of sequences derived under this heading are nonlinear in the sense that the sequences in a family are not closed under pointwise addition. The linear complexity (LC) of a sequence is the shortest length linear feedback shift register which generates the sequence. Even though nonlinear property hinders the evaluation of correlation parameters, sequences possessing this property are essential in certain environments. In spread spectrum communication systems, apart from the good correlation properties it is desirable to have sequences with large LC.

Evaluation of LC of finite field sequences is greatly facilitated by using Blahut's theorem which says that the LC of a sequence is equal to the number of non-zero terms in the discrete Fourier transform representation of the sequence [10]. An extension of Blahut's theorem for the case of sequences over rings is stated and has been made use of for the computation of LC of sequences over finite rings.

The important results obtained are classified into the following two categories.

1. Generalized Polynomial Sequences
2. Sequences Obtained From Mappings from a Ring to its Ideals

*Generalized Polynomial Sequences:* A generalization of a complexity enhancement procedure for finite field  $m$ -sequences [8] to sequences over residue class rings is presented. This is an extension of the case of polynomial sequences over finite fields. The scheme makes use of generalized permutation polynomials over appropriate Galois extension rings. Two generalizations of permutation monomials over  $GR(4, r)$  are obtained from permutation monomials over  $GF(2^r)$ . These give rise to two families of generalized GMW (GGMW) sequences over  $Z_4$  of period  $2^{ru}-1$ , where  $u$  is a positive integer. The size of the GGMW family is  $2^{ru}+1$ , and the sequence over the ideal  $\langle 0, 2 \rangle$  is isomorphic to binary GMW sequence.

The LC of GGMW sequences is computed and shown to be in the range.

$$\{r(u^{H(b)}), \dots, r(u^{H(b)}) + \frac{(2^{ru}-1)}{(2^r-1)} r\} \quad (7)$$

where  $H(b)$  is the number of ones present in the binary representation of  $b$ ;  $0 \leq b \leq 2^r - 1$ . Correlation properties of these families satisfy Welch bound on inner-products with equality, which implies that the  $\theta_{\text{rms}}$  of sequences of period  $L$  is approximately equal to  $\sqrt{L}$ . However,  $\theta_{\text{max}}$  deviates from optimal value of  $\sqrt{L}$ ; computer results suggest that the frequency of deviation is not large.

A similar procedure for LC enhancement for sequences over  $P_2^n[w^k]$  is also considered and a generalized family of GGMW sequences of period  $2^{ru} - 1$  is obtained. By using a subset of GGMW sequences, families of optimal frequency hopping sequences are constructed. The LC of these sequences is shown to be equal to  $r(u^{H(b)})$ , where  $H(b)$  is as defined in (7). The families satisfy Lempel and Greenberger bound on  $H_{\text{max}}$  [1]. The generalized polynomial families satisfy generalized  $r$ -tuple distribution.

*Sequences Obtained From Mappings from a Ring to its Ideals:* Sometimes, mappings from a ring to its ideals yield useful families of sequences. We consider a nonlinear polynomial ( $\mathcal{NL}$ ) mapping from  $Z_4$  to its ideal  $\langle 2 \rangle$ , given by  $\varphi(x) = x^2 - x$ . This mapping results in sequences over the ideal  $\langle 2 \rangle$  which are structurally different from the sequences over  $Z_4$ . The ideal  $\langle 2 \rangle$  is isomorphic to the binary field and the quadriphase mapping  $\phi$  on the sequences over ideal results in biphasic sequences. The quadriphase families derived in the thesis are used for constructing biphasic sequences. Following two families of biphasic sequences are derived from  $Z_4$  families.

1. Families of biphasic sequences of period  $(2^r - 1)$  derived from  $\mathcal{K}$  families over  $Z_4$ ; each family consisting of  $(2^r + 1)$  sequences.
2. Families of biphasic sequences of period  $2(2^r - 1)$  derived from  $\mathcal{KK}$  families over  $Z_4$ .

A method given in [11] for computing correlation properties of biphasic sequences derived from quadriphase sequences is used to compute correlation properties of the biphasic families of sequences. Most of the families satisfy Sidelnikov bound ( $\theta_{\text{max}} \leq \sqrt{2L}$ ) and Welch bound ( $\theta_{\text{max}} \leq \sqrt{L}$ ) on correlations. The LC of the sequences is computed and is shown to be quadratic in  $r$ , where  $r$  is the degree of extension ring used to construct the sequences.

## II. Families derived from the representation of semi-local rings

Families derived under this heading are useful in slow frequency hopping spread spectrum (SFHSS) systems. In SFHSS systems, one or more symbols are transmitted within one frequency hop (slot) and a hit would mean total loss of data transmitted in that hop. Thus, apart from minimizing the mutual Hamming correlation between patterns, hits resulting from presence of all the sequences in the system should be

minimized. This implies that sequences should have good generalized Hamming correlation properties (Eqs (3) & (4)). By utilizing properties of orthogonal ideals of polynomial residue class ring, and families derived over local rings, we construct families of sequences over semi-local rings having ideal GHCC (crosscorrelation function is equal to zero for all values of  $\tau_i$ ). The construction is mainly based on the internal direct sum representation of the ring  $P_p^n[w(\xi)]$ . Following new families are derived.

1. A family of  $p^{n_2}$  sequences of period  $L = p^{n_1-1}$  over  $P_p^n[w(\xi)]$ , where  $n = n_1 + n_2$ , by using a sequence over  $P_p^{n_1}[w_1(\xi)]$  of period  $p^{n_1-1}$ , where  $w_1(\xi)$  is an irreducible factor (of degree  $n_1$ ) of  $w(\xi)$ . These sequences satisfy ideal GHCC properties.
2. A family of  $\mu p^{n_2}$  sequences of period  $L = p^{n_1-1}$  over  $P_p^n[w]$ ,  $n = n_1 + n_2$ , by using  $\mu$  one-coincidence sequences over  $P_p^{n_1}[w_1(\xi)]$  each of period  $p^{n_1-1}$ . The GHCC and GHAC for any sequence in the family are given by

$$\begin{aligned} \text{GHAC}_m(\tau_1, \tau_2, \dots, \tau_{m-1}, \tau_{m+1}, \dots, \tau_n) &\leq p^{n_1-1} - \mu \text{ for } \tau_j = 0 \\ &\leq \mu - 1 \text{ otherwise.} \end{aligned}$$

$$\text{GHCC}_m(\tau_1, \tau_2, \dots, \tau_n) \leq \mu - 1 \text{ for all } \tau_i \neq \tau_j.$$

A code generation scheme, based on the direct sum decomposition of semi-local rings, for slow hopping multiple access communication systems is given where different users can have different frequency diversity.

## REFERENCES:

1. M. K. Simon, J. K. Omura, R. A. Scholtz, B. K. Levit, "Spread Spectrum Communications", Vol 1, Computer Science Press, 1985.
2. D. Sarwate, M. Pursley, "Crosscorrelation Properties of Pseudo random and related Sequences", Proc. of the IEEE., May 1980, p 593-619.
3. S. W. Golomb, Shift Register Sequences, Holden-Day, San Francisco, 1967.
4. P. Sole, "A Quarternary Cyclic Code, and a Family of Quadriphase Sequences with Low Correlation Properties", Coding theory and applications, Lecture Notes in Comp. Sc. vol 388. 1989.
5. W. S. Jibrail and A. R. J. Houmadi, "Acquisition of Direct Sequence Spread Spectrum Signals using Sliding Correlators", Int. J. Electronics, Vol 71, No 5, 1991, pp 733-743.
6. Hari Bhat, "Linear Sequential Systems over Residue Class Polynomial Rings: Theory and Applications", Ph.D thesis, Department of Electrical Engineering, I.I.T, Kanpur, 1985.
7. Serdar Boztas, R. Hammons, and P. V. Kumar, "Near-Optimal Sequences for CDMA", IEEE Trans Inform. Theory, Vol IT-38, No 3 May 1992, pp 1101-1113.
8. T. Siegenthaler and R. Forre, "Generation of Binary Sequences with Controllable Complexity and Ideal r-tuple Distribution", EUROCRYPT-85, Lecture Notes in Comp. Sc. vol 219, 1985.
9. J. J. Komo and S. C. Liu, "Maximal Length Sequences for Frequency Hopping", IEEE Journal on Selected Areas in Communications, Vol 8, No 5, June 1990, pp 819-822.
10. J. L. Massey and T. Schaub, "Linear Complexity in Coding Theory", Coding Theory and Applications, Lecture Notes in Comp. Sc. vol 311. 1988
11. S.M.Krone, D.V. Sarwate, "Quadriphase Sequences for Spread-Spectrum Multiple-Access Communication", Vol IT-30, No 3 May 1984, pp 520-529.
12. J. L. Massey, "On Welch's Bound for the Correlation of a Sequence Set", IEEE Int. Symp. Inform. Theory, Budapest, Hungary, June 24-28, 1991, pp 385.

Table 1. Ring Structures Matched to Correlation Functions

Sl No	Matched Ring	Correlation type	Mapping	$f(a,b)$ .
1.	$Z_M$	M-ary IP Type	$\phi: Q \rightarrow C$ $\phi(a) = \exp(\frac{j2\pi\phi'(a)}{M})$ $\phi': Q \rightarrow Z_M$	$ab^*$
2.	$Z_2 \equiv GF(2)$	Binary IP Type	$\phi: Q \rightarrow R$ $\phi(a) = (-1)^{\phi'(a)},$ $\phi': Q \rightarrow Z_2$	$ab$
3.	$Z_4$	QPSK IP Type	$\phi: Q \rightarrow C$ $\phi(a) = (\omega)^{\phi'(a)},$ $\phi': Q \rightarrow Z_2$	$ab^*$
4.	Any Ring	Hamming	$\phi: Q \rightarrow Q'$	$= 1, \text{ if } a = b$ $= 0, \text{ otherwise}$
5.	$Z_M$	Lee	$\phi: Q \rightarrow Z_M$	$\lfloor M/2 \rfloor - \text{Lee}(a,b)$ $\text{Lee}(a,b) = \min\{ a-b ,  b-a \}$
6.	$P_p^n[w]$	Block Inner-Product type (p-ary)	$\phi^B: q^r \rightarrow C^r$ $A = (a_1 \dots a_r),$ $\phi^B(A) = \phi(a_1) \dots \phi(a_r)$ $\phi(a) = \exp(\frac{j2\pi\phi'(a)}{p}), \phi': Q \rightarrow Z_p$	$A^T \cdot B^*$ T: transpose ·: dot-product
7.	$P_p^n[w]$	Block Hamming	$\phi: q^r \rightarrow q'^r$ $A = (a_1 \dots a_r)$	$F(A,B) = \sum_{i=0}^r f(a_i, b_i)$ where f is as in 4.

# TABLE OF CONTENTS

	Page
LIST OF TABLES	xxiii
LIST OF FIGURES	xxvii
LIST OF SYMBOLS AND ABBREVIATIONS	xxviii
 Chapter 1      Introduction	 1
1.1      Structural Approach for Construction of Sequences over Finite Rings	 2
1.2      Finite Rings Matched to Signal Sets for Correlation	5
1.3      Main Results	10
1.4      Literature Survey	19
1.5      Organization of the Thesis	22
 Chapter 2      Correlation and Related Properties of Sequences over Residue Class Integer and Polynomial rings	 25
2.1      Generalized Correlation Function	26
2.2      More on Finite Rings Matched to Signal Set for Correlation	 31
2.3      Equivalence of Correlation Functions	34
2.4      A Generalized Hamming Correlation Function	36
2.5      Criteria for Signal Design in Communication Systems	37
2.5.1      Inner-product Correlations	37
2.5.2      Hamming Correlation	40
2.5.3      Linear Complexity	41

Chapter 3	Maximal Length and Allied Sequences over $Z_4$ and $Z_8$	43
3.1	Salient Features of Galois Ring $GR(4,r)$	43
3.2	Association Schemes on Abelian Groups	46
3.2.1	Characters of Finite Abelian Groups	47
3.2.2	An Association Scheme Defined on the Elements of $GR(4,r)$	48
3.3	Trace Sequence Families over $Z_2^k$	51
3.4	Families of Maximal-length Sequences over $Z_4$	52
3.4.1	Number of Cyclically Equivalent Families	52
3.4.2	Correlation Computations of m-sequences over $Z_4$	54
3.4.3	Correlation Distribution	61
3.5	Families of Interleaved m-sequences	61
3.5.1	Number of Distinct Families	62
3.5.2	Correlation Computation	62
3.5.3	Correlation Distribution	74
3.6	Maximal Length Sequences over $Z_8$	74
3.6.1	Construction of octaphase sequences	74
3.6.2	Sequence Sets Satisfying Welch's Bound With Equality	76
3.6.3	Number of Distinct Octo-phase Sequence Sets	77
3.6.4	Correlation computations of m-sequences over $Z_8$	77
Chapter 4	Maximal Length Sequences over Local Residue Class Polynomial Rings	81
4.1	Vector Space Structure of $P_p^n[w^k]$ and $PGR(V^k, r)$	81
4.1.1	Representations of $P_p^n[w^k]$	81
4.1.2	Representations of $PGR(V^k, r)$	83
4.2	Trace Sequence Families	85
4.3	Families of Maximal Length Sequences over $P_p^n[w^k]$	86
4.3.1	Number of Distinct Families of m-sequences	87



4.4	Hamming Correlation Properties of $m$ -sequences over $P_p^n[w^k]$	88
4.4.1	Properties of $m$ -sequences over Finite Field	88
4.4.2	Hamming Autocorrelation Properties of $m$ -sequences over $P_p^n[w^k]$	89
4.5	Sets of Frequency Hopping Patterns Derived from $m$ -sequences over $P_p^n[w^k]$	90
4.5.1	Optimal Families of Sequences over $P_p^n[w^k]$	91
4.5.2	Frequency Hopping Patterns from $\mathcal{K}(A)$	92
4.5.3	Number of Families of Frequency Hopping Patterns	92
4.6	$m$ -sequences Having Ideal Block Inner-product Autocorrelations.	96
4.6.1	Block $p$ -phase Sequences from $P_p^n[w^k]$ Sequences	96
4.6.2	Block Inner-product Autocorrelations of $m$ -sequences over $P_p^n[w^k]$	96
Chapter 5	Controllable Large Linear Complexity Sequences over $Z_4$ and Local Residue Class Polynomial Rings	98
5.1	Permutations over $GR(4,r)$ and $PGR(V^k,r)$	98
5.1.1	Permutations over $GR(4,r)$	99
5.1.2	Permutations over $PGR(V^k,r)$	101
5.2	General Procedure for Obtaining Sequences with Large Linear Complexity	101
5.2.1	Procedure for Sequences over Finite Field Complexity Enhancement using Permutation Monomials:	101
5.2.2	Extension to Local Residue Class Rings $Z_4$ and $P_p^n[w^k]$	103
5.3	Generalized GMW (GGMW) Sequences over $Z_4$ and $P_p^n[w^k]$	105
5.3.1	GGMW Sequences over $Z_4$	105
5.3.2	GGMW Sequences over $P_p^n[w^k]$	108
5.3.3	Generalized $r$ -tuple Distributions	108

5.4	Properties of Families of GGMW Sequences over $Z_4$	109
5.4.1	GGMW Families Satisfying Welch bound with Equality	110
5.4.2	Autocorrelation and Crosscorrelation Properties of GGMW Sequences	112
5.4.3	Generalized Auto Correlation Properties of GGMW Sequences	113
5.4.4	Linear Complexity Computation	116
5.5	Properties of Families of GGMW Sequences over $P_p^n[w]$	120
5.5.1	Hamming Correlation Computation of a Subgroup of GGMW Sequences	121
5.5.2	Construction of Optimal Families of Sequences from GGMW Sequences over $P_p^n[w^k]$	123
5.5.3	Sets of Frequency Hopping Patterns from Optimal Families of GGMW( $A$ ) Sequences	124
5.5.4	Linear Complexity of GGMW Sequences $P_p^n[w^k]$	124
Chapter 6	Sequences over the Proper Ideal of $Z_4$ with Controllable Linear Complexity	128
6.1	Polynomial Mappings from $Z_4$ to $\langle 2 \rangle$	129
6.2	Correlation Expressions for Biphase Sequences	130
6.3	Families of $\mathcal{NLP}$ Sequences Derived from $\mathcal{K}$ Families over $Z_4$	131
6.3.1	Weight Distribution of $\mathcal{K}$ - $\mathcal{NLP}$ Family	131
6.3.2	Correlation Distribution of $\mathcal{NLP}$ - $\mathcal{K}$ families	132
6.4	Families of $\mathcal{NLP}$ Sequences Derived From $\mathcal{JK}$ Families	134
6.4.1	Weight and Correlation Transform Distributions	135
6.4.2	Correlation Distribution of $\mathcal{NLP}$ - $\mathcal{JK}$ families	138
6.5	Linear Complexity Computation of $\mathcal{NLP}$ Sequences	142
6.6	Comparison of New Biphase Constructions with Known Families	150

Chapter 7	Sequences over Semi-local Residue Class Polynomial Rings	153
7.1	Slow Frequency Hopping Multiple Access Communication Systems	153
7.1.1	Correlation Requirements on the Patterns	157
7.2	Construction of Frequency Hopping patterns from Sequences over Orthogonal Ideals of $P_p^n[w(\xi)]$	158
7.2.1	Construction of Sequences with Ideal Generalized Hamming Correlation Properties	159
7.3	Construction of Set of Hopping Patterns over $P_p^n[w(\xi)]$ from One-coincidence Sequences over $P_p^n[w_1]$	161
7.4	Construction of Sequences with Variable Frequency Expansion Factors	163
Chapter 8	Conclusions	168
8.1	Summary of Results	168
8.2	Suggestions for Further Work	172
Appendix A	Properties of $Z_{2^k}$ and $GR(2^k, r)$	175
Appendix B	Automorphisms and Trace functions of $GR(2^k, r)$	178
Appendix C	Irreducible Polynomials over $Z_4$ and $Z_8$	181
Appendix D	Properties of $P_p^n[w^k]$ and $PGR(V^k, r)$	185
Appendix E	Sequence Sets Satisfying Welch's Bound with Equality	190
Appendix F	Internal Direct Sum Representation of $P_p^n[w(\xi)]$	192
REFERENCES		193

# LIST OF TABLES

Table No.		Page
1.2.1	Comparison Between $Z_4$ and $GF(2^2)$ Alphabets for Quadriphase Sequence Design	9
1.3.1	Some Parameters of m-sequences over $Z_2$ and $Z_4$	12
2.1.1	Table of Correlation Functions & its Corresponding Distance Measures	32
2.2.1	Ring Structures Matched to Correlation Functions	35
3.4.1	Correlation Transform Distribution of All Phases of m-sequences over $Z_4$ of Period $2^r-1$	55
3.4.2	Correlation Transform and Weight Distributions of m-sequences of Period $2^r-1$	58
(a)	r: odd integer, $r = 2t+1$	58
(b)	r: even integer, $r = 2t$	58
3.4.3	m-sequences of Period 7 (Example 3.4.1)	59
3.4.4	m-sequences of Period 15 (Example 3.4.2)	60
3.4.5	Crosscorrelation Distribution of $\mathcal{K}$	61
3.5.1	Correlation Transform and Weight Distributions of $\mathcal{K}^\gamma(\text{tr}(\tilde{\gamma})=1)$	68
(a)	r: Odd Integer, $r = 2t+1$ ; Period = $2(2^r-1)$	68
(b)	r: Even Integer, $r = 2t$ ; Period = $2(2^r-1)$	68
3.5.2	Correlation Transform and Weight Distributions of $\mathcal{K}^\gamma(\text{tr}(\tilde{\gamma})=0)$	69
(a)	r: Odd Integer, $r = 2t+1$ ; Period = $2(2^r-1)$	69
(b)	r: Even Integer, $r = 2t$ ; Period = $2(2^r-1)$	69
3.5.3	Correlation Transform and Weight Distributions of $\mathcal{K}^\gamma(\gamma = 3)$	70
(a)	r: Odd Integer, $r = 2t+1$ ; Period = $2(2^r-1)$	70
(b)	r: Even Integer, $r = 2t$ ; Period = $2(2^r-1)$	70

3.5.4	$\mathcal{KK}$ Families of Period 30 (Example 3.5.1)	71
a.	Sequences of Family $\mathcal{KK}^{\gamma}(\text{tr}(\bar{\gamma}) = 1; \gamma = (1002)$	71
b.	Sequences of Family $\mathcal{KK}^{\gamma}(\text{tr}(\bar{\gamma}) = 0; \gamma = (1200)$	71
c.	Sequences of Family $\mathcal{KK}^{\gamma}(\gamma = 3)$	72
3.5.5	$\mathcal{KK}$ families of period 62 (Example 3.5.2)	72
a.	Sequences of family $\mathcal{KK}^{\gamma}(\text{tr}(\bar{\gamma}) = 1; \gamma = (32000)$	72
b.	Sequences of Family $\mathcal{KK}^{\gamma}(\text{tr}(\bar{\gamma}) = 0; \gamma = (12000)$	73
c.	Sequences of Family $\mathcal{KK}^{\gamma}(\gamma = 3)$	73
3.5.6	Properties of Quadriphase Families	75
3.6.1	Sequences of $\mathcal{K}(\bar{a})$ , for All $\bar{a} \in \{G_c \cup 0\}$	78
a.	Family $\mathcal{K}(\bar{a})$ ; $\bar{a} = (010)$	78
b.	Family $\mathcal{K}(\bar{a})$ ; $\bar{a} = (001)$	79
c.	Family $\mathcal{K}(\bar{a})$ ; $\bar{a} = (132)$	79
d.	Family $\mathcal{K}(\bar{a})$ ; $\bar{a} = (277)$	79
e.	Family $\mathcal{K}(\bar{a})$ ; $\bar{a} = (775)$	80
f.	Family $\mathcal{K}(\bar{a})$ ; $\bar{a} = (561)$	80
g.	Family $\mathcal{K}(\bar{a})$ ; $\bar{a} = (100)$	80
h.	Family $\mathcal{K}(\bar{a})$ ; $\bar{a} = (000)$	80
4.1.1	Various Representations of $P_p^n[w^k]$	82
4.1.2	Elements of $P_2^4[(1+\xi+\xi^2)^2]$ in Different Representations	83
4.1.2	Representations of $PGR(V^k, r)$	84
4.3.1	m-sequences of Example 4.3.1	87
4.5.1	Weight Distribution of Zeroth Level m-sequences	94
4.5.2	$\#(r, \rho)$ for $r = 2, 3, 4, 5, 6$	94
4.5.3	Number of Frequency Hopping Families Obtained from Zeroth Level m-sequences over $P_p^n[w^r]$ of Period $V^r - 1$	95
4.5.4	Frequency Patterns of Family $\mathcal{K}(1 + (\xi^2)\alpha + (\xi)\alpha^2)$ (Example 4.5.1)	95

5.4.1	Autocorrelation Values of a Prime GGMW Sequence $S^1$	113
5.4.2	Linear Complexity Properties of GGMW Sequences of Period 63	120
5.5.1	Patterns of Family GGMW $((10)+(01)\alpha+(01)\alpha^2+(01)\alpha^3)$	127
6.1.1	Table of Mappings from $Z_4$ to $\langle 2 \rangle \cong GF(2)$	129
6.3.1	Weight and Correlation Transform Distributions of $\mathcal{NLS}\text{-}\mathcal{M}$ Family	132
a.	Period : $2^r-1$ , $r$ an Odd Integer; $r = 2t+1$	132
b.	Period : $2^r-1$ , $r$ an Even Integer; $r = 2t$	132
6.3.2.	Correlation Distribution of $\mathcal{NLS}\text{-}\mathcal{M}$ Family	135
a.	Period: $2^r-1$ , $r$ an Odd Integer; $r = 2t+1$	135
b.	Period: $2^r-1$ , $r$ an Even Integer, $r = 2t$	135
6.4.1	Weight and Correlation Transform Distributions of $\mathcal{NLS}\text{-}\mathcal{M}(\text{tr}(\tilde{\gamma})=1)$ Families	136
a.	Period $2(2^r-1)$ , $r$ an Odd Integer; $r = 2t+1$	136
b.	Period $2(2^r-1)$ , $r$ an Even Integer; $r = 2t$	136
6.4.2	Weight and Correlation Transform Distributions of $\mathcal{NLS}\text{-}\mathcal{M}(\text{tr}(\tilde{\gamma})=0)$ Families	136
a.	Period $2(2^r-1)$ , $r$ an Odd Integer; $r = 2t+1$	136
b.	Period $2(2^r-1)$ , $r$ an Even Integer; $r = 2t$	137
6.4.3	Weight and Correlation Transform Distributions of $\mathcal{NLS}\text{-}\mathcal{M}(\gamma=3)$ Families	137
a.	Period $2^r-1$ , $r$ an Odd Integer; $r = 2t+1$	137
b.	Period $2^r-1$ , $r$ an Even Integer, $r = 2t$	137
6.4.4	Crosscorrelation Distribution of $\mathcal{NLS}\text{-}\mathcal{M}(\text{tr}(\tilde{\gamma})=1)$ Family	140
a.	Period $2(2^r-1)$ , $r$ an Odd Integer; $r = 2t+1$	140
b.	Period $2(2^r-1)$ , $r$ an Even Integer, $r = 2t$	140

6.4.5.	Correlation Distribution of $\mathcal{NLP}\text{-}\mathcal{IK}^{\gamma}(\text{tr}(\tilde{\gamma})=0)$ Family	141
a.	Period $2(2^r-1)$ , $r$ an Odd Integer; $r = 2t+1$	141
b.	Period $2(2^r-1)$ , $r$ an Even Integer, $r = 2t$	141
6.4.6	Correlation Distribution of $\mathcal{NLP}\text{-}\mathcal{IK}^3$ Family	142
a.	Period $2(2^r-1)$ , $r$ an Odd Integer; $r = 2t+1$	142
b.	Period $2(2^r-1)$ , $r$ an Even Integer, $r = 2t$	142
6.5.1	Linear Complexity Distribution of $\mathcal{NLP}$ Sequences	144
6.5.2	Sequences of $\mathcal{NLP}\text{-}\mathcal{IK}$ of Period 7 (Example 6.5.1)	145
6.5.3	Sequences of $\mathcal{NLP}\text{-}\mathcal{IK}$ of Period 15 (Example 6.5.2)	146
6.5.4	$\mathcal{NLP}$ Families of Im-sequences of Period 30 (Example 6.5.3)	147
a.	Sequences of Family $\mathcal{NLP}\text{-}\mathcal{IK}^{\gamma}(\text{tr}(\tilde{\gamma}) = 1; \gamma = (1002)$	147
b.	Sequences of Family $\mathcal{NLP}\text{-}\mathcal{IK}^{\gamma}(\text{tr}(\tilde{\gamma}) = 0; \gamma = (1200)$	147
c.	Sequences of Family $\mathcal{NLP}\text{-}\mathcal{IK}^{\gamma}(\gamma = 3)$	148
6.5.5	$\mathcal{NLP}\text{-}\mathcal{IK}$ Families of Period 62 (Example 6.5.4)	148
a.	Sequences of Family $\mathcal{NLP}\text{-}\mathcal{IK}^{\gamma}(\text{tr}(\tilde{\gamma}) = 1; \gamma = (32000)$	148
b.	Sequences of Family $\mathcal{NLP}\text{-}\mathcal{IK}^{\gamma}(\text{tr}(\tilde{\gamma}) = 0; \gamma = (12000)$	149
c.	Sequences of Family $\mathcal{NLP}\text{-}\mathcal{IK}^{\gamma}(\gamma = 3)$	149
6.6.1	Comparison of New Biphase Sequence Constructions with Previously Known Families	151
6.6.2	Optimality Properties of Quadriphase and Biphase families under $\mathcal{NLP}$ Mapping	152
7.2.1	Sequences for Example 7.2.1	160
C1	All Basic Monic Irreducible Polynomials over $\mathbb{Z}_4$ of degree $r$ ; $r = 3$ and $4$	181
C2	All Basic Monic Irreducible Polynomials over $\mathbb{Z}_8$ of degree $r$ ; $r = 3$	182
C3	Basic Irreducible Polynomials over $\mathbb{Z}_4$ of Degree $r$ ; $r = 5, 6, 7, 8, 9$ Such that Exponent Divides $2^r-1$	183

# LIST OF FIGURES

Fig. No.		Page
1.1.1	Structural Approach for Construction of Sequences	3
2.2.1	Relation between Matched Rings and Signal Sets	34
2.5.1	LFSR of Length $m$	41
3.4.1	Schematic Diagram of $m$ -sequence Generation over $Z_4$	53
4.5.1	Schematic Diagram of Generation of Frequency Hopping Patterns using $m$ -sequences over $P_p^n[w^k]$	92
5.3.1	Schematic Diagram of Generation of Quadriphase Sequences Derived from GGMW Sequences	106
5.4.1	Autocorrelation Distribution of Selected GGMW sequences of Period 63 (Example 5.4.1)	114
5.4.2	Crosscorrelation Distribution of GGMW sequences of Period 63 (Example 5.4.1)	114
5.4.3	Autocorrelation Distribution of Selected GGMW sequences of Period 255 (Example 5.4.2)	115
5.4.4	Distribution of Correlation Values between $S^1$ and all GGMW sequences of Period 255 (Example 5.4.2)	115
5.5.1	Schematic Diagram of Generation of Frequency Hopping Patterns from GGMW Sequences over $P_p^n[w^k]$	125
6.3.1	Schematic Diagram for Generation of Biphasic Sequences from Sequences Over $Z_4$	131
7.1.1	Slow Frequency Hopping Spread Spectrum System	155
a.	Transmitter	155
b.	Receiver	155
7.1.2	Time-frequency Graph of the Baseband Signal	156
7.1.3	Time-frequency Graph of the Transmitted Signal for Example 7.1.1	156
7.2.1:	A Code Generation Arrangement for Slow Hopping M-A Communication Environment	161
7.4.1	Code Generation Arrangement for Slow Hopping M-A system with Users Having different Frequency Expansion Factors	165



# LIST OF SYMBOLS AND ABBREVIATIONS

$L$	:	Period.
$\mathcal{A}$	:	Finite alphabet.
$\mathcal{R}$	:	Finite ring.
$Z_{2^k}$	:	Residue class integer ring modulo $2^k$ , $k$ being a positive integer.
$P_p^n[w(\xi)]$	:	Residue class polynomial ring $GF(p)[\xi] \bmod w(\xi)$ , where $w(\xi)$ is an $n^{\text{th}}$ degree polynomial over $GF(p)$ .
$P_p^n[w]$	:	Symbol for $P_p^n[w(\xi)]$ .
$P_p^n[w^k]$	:	Local $P_p^n[w]$ ring.
$SP_p^m[w]$	:	Subfield of $P_p^n[w^k]$ .
$GR(2^k, r)$	:	Galois extension ring of $Z_{2^k}$ of degree of extension $r$ .
$PGR(V^k, r)$	:	Galois extension ring of $P_p^n[w^k]$ of degree of extension $r$ .
$GR^*(2^k, r)$	:	Group of units of $GR(2^k, r)$
$PGR^*(V^k, r)$	:	Group of units of $PGR(V^k, r)$ .
$G_a$	:	Abelian group of units of Galois extension rings
$G_c$	:	Cyclic group of units of Galois extension rings
$SPGR(V, r)$	:	Subfield of $PGR(V^k, r)$
$(\cdot : \text{reduction modulo } 2)$	:	ring homomorphism from $GR(4, r)$ to $GF(2^r)$
$-$	:	Denotes isomorphic mapping from $G_a$ of $GR(4, r)$ to $GF(2^r)$
$U$	:	Set theoretic union

$\text{tr}_1^r$	:	Trace function from $r^{\text{th}}$ degree Galois extension ring to its ground ring
$\chi$	:	Characters of finite Abelian group
$X$	:	Classes of Association scheme
$\text{TRACE}(A)$	:	Sum of all diagonal elements of the matrix $A$
$< 2 >$	:	Proper ideal of $Z_4$
$\otimes$	:	Direct product
$\oplus$	:	Direct sum
$\equiv$	:	isomorphic to
$\in$	:	belongs to
$\square$	:	end of proof
$(a,b)$	:	$a$ is relatively prime to $b$
$f$	:	Correlation operation
$\phi$	:	Mapping from $\mathcal{A}$ to Signal set
$\phi$	:	Euler's $\phi$ function.
$\text{IP}$	:	Inner-product
$\text{BIP}$	:	Block Inner-product
$\mathcal{K}^{(f,\phi)}(A)$	:	Correlation transform of a sequences $A$ corresponding correlation function represented by $(f,\phi)$
$\mathcal{K}$	:	Correlation transform
$C_{AB}(\tau)$	:	Correlation Function
$(.)^*$	:	Complex conjugate of $(.)$
$(.)^T$	:	transpose of $(.)$
$\cdot$	:	dot product.
$\text{Lee}(a,b)$	:	Lee distance between $a$ and $b$ which is equal to minimum $ a-b $ or $ b-a $ ; $  \cdot  $ is the mod symbol.

GCH	:	Generalized Hamming Crosscorrelation Function.
GAH	:	Generalized Hamming autocorrelation function.
$\mathcal{M}$	:	Family of maximal length sequences.
$\mathcal{IM}$	:	Family of Interleaved maximal length sequences.
$\mathcal{NLP}$	:	Family of Non-linear polynomial sequences.
GGMW	:	Generalized GMW.
SFH	:	Slow frequency hopping.
M-A	:	Multiple Access.
$\Psi$	:	Permutation over a Galois ring.
$\mathbb{F}$	:	Family.
$\theta_{\max}$	:	$\{\text{Max} (C_{XX}(\tau), \tau \neq 0, C_{XY}(\tau) \mid X \neq Y, X, Y \in \mathbb{F})\}.$
$\theta_{\text{rms}}$	:	Mean Square root of $( C_{XY}(\tau) ^2, \text{ for all } X, Y \in \mathbb{F}, \text{ except when } X = Y \text{ \& } \tau = 0).$
$\theta_{\text{avg}}$	:	Average of $ C_{XY}(\tau) $ , for all $X, Y \in \mathbb{F}$ , except when $X = Y \text{ \& } \tau = 0.$

# Chapter 1

## Introduction

This thesis is concerned with algebraic construction of sequences obtained from residue class finite rings and with their periodic correlation and linear complexity (LC) properties. Such sequences are of interest in polyphase and frequency hopping code division multiple access (CDMA) communication systems. The finite rings considered in this study are:

- Residue class integer ring modulo  $2^k$ :  $Z_{2^k}$ ,  $k$  being a positive integer.
- Residue class polynomial ring  $GF(p)[\xi] \bmod w(\xi)$ :  $P_p^n[w(\xi)]$ , where  $w(\xi)$  is an  $n^{\text{th}}$  degree polynomial over  $GF(p)$ .

CDMA communication systems require a large set of sequences, in which each sequence is easily distinguished from every other sequence in the set and from all time shifted versions of itself. The criteria of distinguishability of sequences depends on the type of modulation and the type of channel. Different types of autocorrelation and crosscorrelation functions are defined to meet these requirements in practice [1–4]. For instance, in biphase modulated communication systems, low inner-product correlations of sequences helps in distinguishing sequences at the receiver. Some times, secrecy considerations demand the sequences to be random and to possess large LC [5]. For the construction of required sequences, a wide range of properties which affect the system performance have been considered in literature [6–14]. Since the requirements on sequences differ from problem to problem, approaches to sequence constructions are specific to the problem. The approaches employed to obtain desired sequences in the literature may be classified into the following two categories.

a) Structural approach.

b) Heuristic search approach.

In the structural approach, method of sequence generation is implicit and the properties of sequences are evaluated by making use of results in discrete mathematics. Use of such sequences in practice depends on the properties these sequences possess. In contrast to this, in heuristic search approach, specific requirements on the sequences are formulated first and efficient algorithms (search methods) are employed to find them [15–18]. Finally, symmetries and structures present in the sequences are to be analyzed for their implementation. Former approach relies on the rich mathematics of algebra and geometry where as

the later depends on the available computing power. In the structural approach, evaluation of the properties is the main challenge, where as in the heuristic search approach, determination of the symmetry and the method of generation is the prime task. Heuristic search methods are employed mainly to find short sequences with minimum autocorrelation side lobes. When large number of long sequences are required having good mutual crosscorrelation and autocorrelation properties, search methods are often time consuming and difficult to execute. In such situations, structural approach is followed and this approach has yielded many useful results. Search techniques are employed mainly in situations where single sequence is used in the system like radar and sonar applications, estimation of impulse response of a channel. Whereas, structural methodology has been employed in varieties of applications like CDMA communication systems, spread spectrum systems, multiplexing systems, radar pulse compression, system identification. The approach used in this thesis falls in the category of structural approach for construction of sequences over finite residue class rings, and is discussed in Section 1.1.

The sequences in this thesis are viewed as polynomial mappings of trace functions of unit elements of Galois extension rings. The periodic correlation properties (correlation values and their distribution) of sequences over  $Z_4$  are obtained by using an Abelian association scheme on the elements of the Galois extension ring of  $Z_4$ . For sequences over  $Z_8$ , the correlation properties are computed by making use of Galois extension ring of  $Z_8$ . The correlation properties of sequences over residue class polynomial rings have been obtained by utilizing the vector space structure of the polynomial ring and the properties of finite field  $m$ -sequences. The LC of sequences has been computed by using a finite ring version of Blahut's complexity theorem for finite field case.

## 1.1 Structural Approach for Construction of Sequences over Finite Rings

The structural approach used to obtain the desired sequences is shown in Fig 1.1. In this approach, sequences are constructed over a finite alphabet by using a sequence generation mechanism. The finite alphabet is transformed into a subset of real (or complex) space through an appropriate mapping  $\phi$ . This subset of real (or complex) space is referred to as a signal set associated with the finite alphabet. Through the mapping  $\phi$ , the sequences over the finite alphabet are transformed into real (complex) valued signals. A familiar example of such an approach is the generation of biphase pseudo-noise sequences using feedback shift registers [19–20], where the finite alphabet is binary field  $GF(2)$ , the signal set is  $\{1, -1\}$ , mapping  $\phi$  is given by  $\phi(a) = (-1)^a$  and the sequence generation mechanism uses feedback shift registers. Such

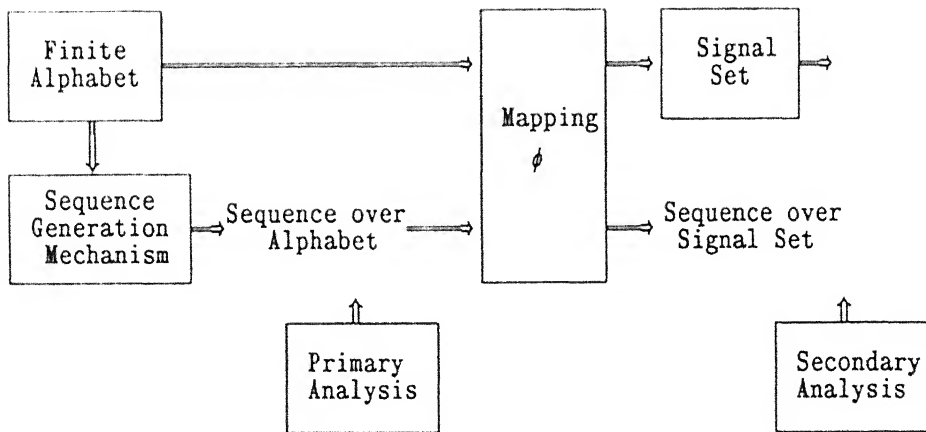


Fig 1.1.1 Structural Approach for Construction of Sequences

sequences have a wide range of applications and there exists a large body of literature dealing with their various aspects.

The sequence generation mechanism is the core of the structural approach. It is dependent on the structure of the alphabet, and is independent of applications. Suitability of generated sequences for any specific application mainly depends on their properties. Hence major effort is required to determine their properties. In the past, various innovative mathematical tools have been used to compute the properties [21–24]. Properties like period, linear complexity, and randomness ( $r$ -tuple distribution, run-length distribution), can be evaluated in the alphabet domain itself; such properties are called primary properties due to their direct dependence on the structure of the alphabet. However, evaluation of correlation properties depends on a mapping  $\phi$  from the alphabet to a signal set; they are termed as secondary properties. The primary properties are better controlled because of their direct dependence on the sequence generation mechanism. However, the same is not true with the secondary properties, although they are more critical in practice. Note that in the structural approach, the sequence design problem is not formulated by stating the constraints on the correlation parameters; it is sheer luck that some of the resulting sequences have nice properties to make them useful in practice.

The structural approach is classified into algebraic or geometric depending on the nature of the sequence generation mechanism. The algebraic approach makes use of the algebraic structure of the

alphabet for sequence generation, whereas in the geometric approach the theory of finite geometry is made use of for construction of sequences. In both approaches, evaluation of primary and secondary properties uses similar analytical tools.

This study is on the lines of the algebraic approach to sequence construction. Most of the existing algebraic sequence generation methods in the literature assume that the sequence alphabet is a finite field. This restricts the alphabet size and the sequence generation mechanism. Finite rings, which are a natural generalization of finite fields, have rich structural properties which can be utilized for sequence generation. In this thesis, the scope of the algebraic sequence construction theory is enlarged by considering residue class finite rings as the sequence alphabet.

The generalization of sequence alphabet from finite fields to residue class rings yields lot of flexibility in choosing primary properties. Moreover, because of its specific properties, a finite ring structure is more suited to some communication systems. Some of the factors which favours the study of sequences over rings are given below.

**Size constraint:** When a finite field is considered as the alphabet for sequence construction, the size of the finite field is restricted to a prime or power of a prime number. Some communication systems, like M-PSK modulated systems, demand alphabet of size other than prime or a prime power. In such cases, a finite ring structure can provide a suitable alphabet. Also, in some modulation schemes which involve large alphabets of size greater than two, finite rings can offer a much wider choice of alphabet size compared to finite fields.

**Flexibility in period length:** The period  $L$  of most of the algebraic sequences generated over finite fields is such that  $L$  divides  $V^r - 1$ , where  $V$  is the field cardinality and  $r$  is the degree of Galois field extension. This is because of the fact that the non-zero elements (units) of the  $r^{\text{th}}$  degree Galois extension field  $GF(V^r)$  constitute a cyclic group of order  $V^r - 1$ ; the multiplicative order of elements in Galois extension field determines the period. In this respect finite rings offer more flexibility, since the group of units of Galois extension rings is in general Abelian. For example, for sequences over  $Z_4$ , we can have periods  $2^r - 1$  and  $2(2^r - 1)$ .

Apart from the advantages cited above, residue class rings are naturally suited for multiplexing operation. Decomposition of rings into internal direct sum of ideals and the fact that the elements belonging to different ideals annihilate each other play an important role in such applications [25]. Using the decomposition of the ring  $P_P^n[w(\xi)]$ , a multiplexing scheme on XOR channel is considered by Hari Bhat

[25]. Nishikado et. al. [26] also have considered a similar scheme using cyclic codes over  $GF(2)$ . These multiplexing schemes are some variants of time division multiplexing, where the message from each source can be multiplexed without being specifically assigned to a particular time slot. In essence, the information due to any source is spread throughout the time slots available. This inherent spreading follows from the structure of the ring. Based on such properties, a spread spectrum system is proposed in [25].

Generalizations of the structure of alphabet give rise to flexibility in choosing primary properties; the same is not true with the secondary properties (correlation properties). Secondary properties have to be analyzed in each case for the suitability of sequences in specific applications. In an attempt to ease the secondary analysis, notion of a sequence alphabet matched to a signal set for a correlation function is proposed.

## 1.2 Finite Rings Matched to Signal Sets for Correlation

The correlation functions are used in many communication systems primarily as a means of measuring the distinguishability of sequences. The type of autocorrelation and crosscorrelation functions to be used mainly depends upon the application where the sequences are used, modulation, and the environment like the type of the channel. Many commonly used correlation functions involve some distance measure in the space of signals where they are used. To take care of various correlation functions of practical importance, a generalized correlation function between a pair of sequences is defined in the thesis such that the specific correlation functions can be derived from it as special cases. The definition of periodic correlation is assumed throughout the thesis.

Let  $A = \{a_0, a_1, \dots, a_{L-1}\}$ ,  $B = \{b_0, b_1, \dots, b_{L-1}\}$  be two sequences of period  $L$  over certain alphabet  $\mathcal{A}$  of size  $|\mathcal{A}|$ . Then the crosscorrelation function  $C_{AB}(\tau)$  between  $A$  and  $B$  is given by

$$C_{AB}(\tau) = \sum_{i=0}^{L-1} f\{\phi(a_i), \phi(b_{(i+\tau) \bmod L})\} ; \tau = 0, 1, \dots, L-1 \quad (1.2.1)$$

where  $\phi$  is a mapping from the finite alphabet  $\mathcal{A}$  to an appropriate signal set which is a subset of real (complex) space, and  $f$  is a binary operation related to the definition of the correlation function which depends on the distance measure. The range of  $f$  is also a subset of real (complex) space. The nature of  $\phi$  and  $f$  depends on the type of modulation and the type of application where the sequences are used. The mapping  $\phi$  which links a finite ring to a signal set may be considered as an abstract modulator. Various correlation functions derived from (1.2.1) and considered in the thesis are binary, quaternary, and  $m$ -ary



inner-product correlations, Hamming and Lee correlations, and block inner-product correlations (a generalized version of inner-product correlations); they are given along with their corresponding distance measures in Table 2.1.1.

Using the generalized correlation function defined above, we introduce the notion of a finite ring matched to a signal set for a given correlation function as follows:

**Definition 1.2.1:** A finite ring  $\mathcal{R}$  is said to be matched to a signal set for correlation represented by a tuple  $(f, \phi)$  if ~~and only if~~

$$f(\phi(a), \phi(b)) = f(\phi(a-b), \phi(0)), \text{ for any } a, b \in \mathcal{R} \quad (1.2.2)$$

where  $-$  denotes the subtraction in the finite ring  $\mathcal{R}$

A simple example of a matched ring is that of a binary field  $GF(2)$  which is matched to biphasic signal set for binary inner-product correlations. In this case, the additive group of  $GF(2)$  is isomorphically mapped to the multiplicative group of  $(1, -1)$  under the mapping  $\phi$ ,  $\phi(a) = (-1)^a$ ;  $(1, -1)$  being the signal set for biphasic signaling.

Some variants of the above concept have been previously considered in the literature in the context of channel coding [27–28]. In these variants, the main idea is to exploit the linearity property of the alphabet domain. Recently, Loeliger [28] has considered signal sets matched to groups. He has proved that  $Z_M$  is matched to  $M$ -PSK signal set.

The main motivation for taking up study of sequences over matched rings is that the computation of correlation properties of sequences over matched rings is greatly simplified by using combinatorial results concerning the correlation transform of sequences, defined below.

**Definition 1.2.2:** The correlation transform of a sequence  $A$  over a finite ring, corresponding to a correlation function characterized by the 2-tuple  $(f, \phi)$ , is defined as the zeroth crosscorrelation between  $A$  and the all 0 sequence  $S^0$ , given by

$$R^{(f, \phi)}(A) = C_{AS^0}(0) = \sum_{i=0}^{L-1} f\{\phi(a_i), \phi(0)\}; \tau = 0, 1, \dots, L-1. \quad (1.2.3).$$

The correlation operation of the signal set is isomorphic to addition in the alphabet structure and more importantly the mapping is linear. This allows us to make use of the linearity of the ring alphabet for the computation of correlations. As a result, generalization of the alphabet structure from finite field to finite ring, in many situations, permits us to retain the advantages of linearity leading to simplicity in the analysis of sequences. Thus, while constructing sequences using the structural approach, it is advantageous

to consider matched ring structures. Further, sequences over matched structures may also have good properties. This belief is strengthened by the existence of optimal sets of quadriphase sequences obtained from  $Z_4$  which is matched to quadriphase signal set for inner-product correlation [29–33].

The motivation for study of sequences over matched rings is well illustrated through an example of quadriphase sequence construction using a finite ring  $Z_4$ . Most of the constructions of quadriphase sequences in the literature are derived either with the assumption that the sequence alphabet is a finite field ( $GF(q)$ ) or based upon the properties of the multiplicative characters of  $GF(q)$  [3]. Moreover, their correlation properties are nowhere near optimal. According to the Welch's lower bound, for a collection of  $L$  complex-valued sequences of period  $L$ ,  $\theta_{\max}$  (the maximum magnitude of periodic crosscorrelation and out-of-phase autocorrelation) cannot be less than a quantity that is approximately  $\sqrt{L}$  [34]. If the alphabet is binary, Sidelnikov has shown that  $\theta_{\max}$  must always exceed  $(2L-2)^{1/2} \cong \sqrt{2L}$  [35] (Sidelnikov bound). While examples of optimal biphasic sequences derived from finite fields are found in literature, finite field constructions of optimal quadriphase constructions do not exist. The  $\theta_{\max}$  results of the quadriphase constructions given in [3] lie faraway from the Welch's bound. These results do not compare well even with binary sequences ( $\theta_{\max} \geq \sqrt{2L}$ ). This gives an impression that finite fields do not constitute a suitable structure for quadriphase signal design. It may be noted that finite fields are not matched to QPSK inner-product correlations. However,  $Z_4$  is a matched ring for quadriphase signal design. To illustrate this point more clearly, let us consider QPSK inner-product correlation function. In this case  $\phi$  is a mapping from a sequence alphabet to the set of 4<sup>th</sup> root of unity and is given by

$$\phi: \mathcal{A} \longrightarrow \mathbb{C} \text{ (Complex field)}, \phi(a) = \exp\left(\frac{j2\pi a'}{4}\right), \quad (1.2.4)$$

where  $a' = \phi'(a)$ ;  $\phi': \mathcal{A} \longrightarrow Z_4$  being another mapping from  $\mathcal{A}$  to  $Z_4$ , and  $f$  is a binary correlation operation defined by  $f(u,v) = uv^*$ ;  $*$  represents complex conjugation. When the sequence alphabet is a finite field, correlation computation of the generated quadriphase sequences depends not only on the finite field but also on the mapping  $\phi'$  which maps the finite field to  $Z_4$ . In most of the cases  $\phi'$  is a non-linear function. i.e.,  $\phi'(a(+)_1 b) \neq \phi'(a)(+)_2 \phi'(b)$ , where  $(+)_1$  and  $(+)_2$  denote addition operations in the alphabets  $\mathcal{A}$  and  $Z_4$  respectively. This makes the correlation computation very tedious. When  $|\mathcal{A}|$  is a power of a prime with exponent greater than 1, the mapping  $\phi'$  is never linear, since additive structure of the finite field with  $|\mathcal{A}|$  elements is not always isomorphic to that of  $Z_4$ . As a result, the sequences are generated in one domain (in this case finite field) and the properties are evaluated based on the mapped sequences over

some other domain ( $Z_4$ ). This may be a possible reason for the nonexistence of optimal quadriphase constructions derived from finite fields. When the finite residue class ring  $Z_4$  is chosen for sequence alphabet, which is matched to QPSK signal for correlation,  $\phi'$  in (1.2.4) is identity and  $f$  becomes  $f(\phi(a), \phi(b)) = \phi(a-b)$ , where  $(-b)$  is the additive inverse of  $b$  in  $Z_4$ . This linear property of  $\phi$  is responsible for the simplification in evaluation of the correlation function. Also from (1.2.2), it is clear that the existence of quadriphase sequences with good correlation properties necessarily implies the existence of good  $Z_4$  sequences. Hence  $Z_4$  is an appropriate structure for quadriphase sequence construction. The only finite field where  $\phi'$  is identity mapping is when  $|A|$  is a prime integer;  $GF(2)$  is one such example which is an appropriate alphabet for biphase constructions. In general, a suitable sequence alphabet used in M-PSK modulated systems is the residue class integer ring  $Z_M$ , wherein the additive structure of  $Z_M$  is isomorphic to the multiplicative structure of  $M^{\text{th}}$  roots of unity. This indicates a close relationship between the mapping considered in the correlation definition and the sequence alphabet. Thus, investigation of sequences over matched structures is worthwhile. Comparison of main features of sequence constructions over the ring  $Z_4$  and the finite field  $GF(2^2)$  are given in Table 1.2.1.

The mapping  $\phi$  provides a link between a finite ring and a signal set, and it may be considered as an abstract modulator. Most of the practical situations demand sequences to be periodic and the signal alphabet can be assumed to be closed under cyclic shifts. So essentially cyclic modules over finite rings are of interest in this context. We have considered several examples of finite residue rings matched to different signal sets for various correlations. Table 2.2.1 gives different examples of residue rings matched to signal sets for various correlations.

From the arguments in the preceding paragraphs, it is seen that finite rings, as alphabets for sequence constructions, provide a much wider choice compared to the finite fields with respect to the choice of length, characteristic, and the appropriateness to correlation.

The generalized correlation function defined by (1.2.1) depends on a pair of sequences. Some communication practices demand correlation function which depends on all the sequences employed in the system. We have considered such correlation functions, called generalized Hamming correlation functions. They are useful in slow frequency hopping multiple access communication systems. They are given as follows.

Let  $S^i$ ,  $m = 1, \dots, n$ , be  $n$  sequences of length  $L$  over certain alphabet  $Q$ , then the generalized Hamming crosscorrelation function concerning  $m^{\text{th}}$  sequence is given by

$$\text{GCH}_m(\tau_1, \tau_2, \dots, \tau_{m-1}, \tau_{m+1}, \dots, \tau_n) = \sum_{i=0}^{L-1} \text{gh}\{S_i^m; S_{i+\tau_j}^j, \text{ for all } j \neq m\}. \quad (1.2.5)$$

The corresponding autocorrelation function is given by

$$\text{GAH}_m(\tau_1, \tau_2, \dots, \tau_n) = \sum_{i=0}^{L-1} \text{gh}\{S_i^m; S_{i+\tau_j}^j, \text{ for all } j\} \quad (1.2.6)$$

where  $\text{gh}$  is a function given by

$$\begin{aligned} \text{gh}\{a; b_1, b_2, \dots, b_n\} &= 1 \text{ if } a \in \{b_1, b_2, \dots, b_n\} \\ &= 0 \text{ other wise.} \end{aligned}$$

Equivalences of some correlation functions are also discussed in the thesis. Two correlation functions are equivalent if the computation of correlation values from one type is sufficient to determine the correlation values from the equivalent correlation function. Familiar examples of equivalent correlation functions are that of binary inner-product correlation and binary Hamming correlation. The equivalence of correlation functions is responsible for efficient digital implementation of some binary synchronization schemes based on Hamming correlation [36]. However, very few correlation functions with such a property exist. Extending the binary field results, binary block inner-product correlation is shown to be equivalent to binary block Hamming correlation.

Table 1.2.1:

Comparison Between  $Z_4$  and  $\text{GF}(2^2)$  Alphabets for Quadrphase Sequence Design

Possible Features	$Z_4$	$\text{GF}(2^2)$
Algebraic sequences with		
a. period $2^r-1$	Yes	Yes
b. period $4^r-1$	Yes	Yes
c. period $2(2^r-1)$	Yes	No
Matched ring for quadrphase correlation	Yes	No
Characteristic = 2	Yes	Yes
= 4	Yes	No
Examples of families satisfying the Welch bound on $\theta_{\max}$	Yes	No (Not Reported)

### 1.3 Main Results

Mainly local rings have been considered in the study since any general semi-local ring can be expressed as a direct sum of local rings. Properties of Galois extension rings of local finite residue class rings  $Z_{2^k}$  and  $P_p^n[w^k]$ , where  $w^k$  denotes  $k^{\text{th}}$  power of an irreducible polynomial  $w(\xi)$  of degree  $m$  over  $GF(p)$  and  $n = mk$ , are used to generalize sequence generation procedures from their finite field counterparts. Galois extension rings here play a role similar to those of Galois extension fields in the case of finite fields. Two important Galois extension rings considered in the thesis are

- Galois extension ring of  $Z_{2^k}$  of degree of extension  $r$ , denoted by  $GR(2^k, r)$ . It is a set of polynomials over  $Z_{2^k}$  of degree less than or equal to  $r-1$ ; ring addition and multiplication are given by polynomial addition and multiplication modulo *basic monic irreducible polynomial* over  $Z_{2^k}$  of degree  $r$ .
- Galois extension ring of  $P_p^n[w^k]$ , denoted by  $PGR(V^k, r)$ , where  $V$  represents the residue field  $P_p^m[w]$  of order  $p^m$  isomorphic to  $GF(p^m)$ .  $PGR(V^k, r)$  is a set of all polynomials of degree less than or equal to  $r$  over  $P_p^n[w^k]$ ; ring addition and multiplication are polynomial addition and multiplications modulo *basic monic irreducible polynomial* of degree  $r$  over  $P_p^n[w^k]$ .

Various families of sequences derived in the thesis are classified into the following classes.

- I. Families derived from local rings.
- II. Families derived from semi-local rings.

#### I. Families derived from local rings

##### *I(a) Linear Constructions:*

Here the sequences in a family are closed under pointwise ring addition. The familiar trace function representation of sequences over finite fields is generalized. Generalized automorphisms of Galois extension of residue class rings are employed to define a trace function from Galois extension ring to its ground ring. Then for any unit element  $\alpha$  which belongs to Galois extension ring, a family of sequences called trace function sequences (or simply trace sequences) is defined. The sequences in a family are generated as the trace of successive powers  $\alpha$ ; the multiplicative order of  $\alpha$  determines the period of the sequences. The trace sequences are of the form:

$$\{tr(A\alpha^i), i = 0, 1, \dots, L-1, \alpha \in \text{Galois extension ring, } L: \text{multiplicative order of } \alpha\}.$$

Since a local residue ring contains a chain of local ideals, the family of trace sequences over a local ring

also includes families of trace sequences over the ring ideals. The trace sequences over the proper ring are called as zeroth level sequences and the sequences over ideals isomorphic to  $Z_2^\kappa$  or  $P_p^n[w^\kappa]$ ,  $1 \leq \kappa \leq k$ , are denoted as  $(k-\kappa)^{\text{th}}$  level sequences. Thus, altogether there are  $k$  level sequences.

The period of a trace sequence is determined by the multiplicative order of the unit element  $\alpha$  used to define the family, and hence possible periods ( $L$ ) depend upon the structure of the group of units of the appropriate Galois extension ring. In case of finite fields, the group of units of  $GF(V^r)$  is a cyclic group of order  $V^r-1$  and thus period  $L$  of trace sequences over  $GF(V)$  is such that  $L$  divides  $V^r-1$ . The group of units of a Galois extension ring is, in general, Abelian which has a cyclic component group  $G_c$  isomorphic to the group of units of its residue field. For example, the group of units of  $GR(4, r)$ ,  $GR^*(4, r)$  is of order  $2(2^r-1)$  with cyclic component group  $G_c$  of order  $2^r-1$ , which is isomorphic to group of units of  $GF(2^r)$ , the residue field of  $GR(4, r)$ . Thus, period  $L$  of trace sequences over  $Z_4$  is such that  $L$  divides  $2(2^r-1)$ . An unit element  $\alpha$  of the cyclic component group is called a primitive element if its multiplicative order is same as the order of the cyclic component group. The family of trace sequences is called a family of  $m$ -sequences or simply  $\mathcal{A}$  family if the unit element  $\alpha$  used to define the family is a primitive unit element of the Galois extension ring.

Remark 1.3.1: (Comment on the use of name 'maximal length' for  $m$ -sequences over the residue class rings): The nomenclature 'maximal length' is appropriate in case of sequences over a finite field, because the length of any finite field  $m$ -sequence is the largest length possible for any sequence generated by a  $r$ -length feedback shift register. This implies that there exists a nonsingular matrix  $A$ , such that the set of operations on  $x$ ,  $A^n(x)$ ;  $x \in V_{q^r}$ ,  $n \in Z_{q^r}$ , span all the elements of  $V_{q^r}$ , where  $V_{q^r}$  is the set of  $r$ -tuples over  $GF(q)$ . Equivalently, there exists only one non-trivial equivalence class of size  $q^r-1$  induced by the linear transformation operation. Analogously, one would expect the length of  $m$ -sequences over a residue class ring,  $\mathcal{R}$ , of order  $V^k$  to be  $V^r-1$ , where  $V$  is the order of residue field. But there is no equivalence class of size  $V^r-1$  induced by the linear transformation operation on the set of  $r$ -tuples of  $\mathcal{R}$  [37-38]. Thus, here maximal length only means that the ring  $m$ -sequences attain maximal length corresponding to its residue field. It is in this sense that the name of  $m$ -sequence families is coined. The main difference between field and ring  $m$ -sequences is that there is only one cyclically distinct finite field  $m$ -sequence for a primitive element  $\alpha$  of  $GF(V^r)$ , whereas in the ring case there is a family of  $m$ -sequences corresponding to an element  $\alpha$  of the extension ring. Differences in parameters of for  $m$ -sequences over  $Z_2$  and  $Z_4$  are given in Table 1.3.1.

Remark 1.3.2: Various characterizations of  $m$ -sequences over finite field are fairly well known. The same, however, is not true in case of rings and the results are scant. We have followed trace function representation for defining  $\mathcal{K}$  families over residue class rings. Alternative characterizations of  $\mathcal{K}$  family are:

- (1) It is a class of sequences generated by a linear feedback shift register (LFSR) of length  $r$  with a connection polynomial given by the minimal polynomial of a primitive unit element  $\alpha$ .
- (2) It is a set of cyclically distinct codewords in a minimal cyclic code over  $\mathcal{R}$  with parameters block length  $V^r-1$  and dimension  $r$
- (3) It is a set of vectors over  $\mathcal{R}$  of length  $V^r-1$  of dimension  $r$  with non-zero spectral coefficients in one conjugacy class corresponding to a primitive unit element  $\alpha$ .

The above characterizations of  $\mathcal{K}$  families over  $\mathcal{R}$  follow directly from the generalizations of their finite field counterparts. First characterization comes from the theory of linear recurring sequences over  $\mathcal{R}$ . Second and third are consequences of the theory of cyclic codes over  $\mathcal{R}$  in time domain and transform domain respectively [39].

Three important families of sequences derived from  $\mathcal{K}$  families have been obtained. They are classified depending on their properties and the area of applicability.

1. Families of quadriphase sequences derived from  $\mathcal{K}$  families over  $Z_4$ .
2. Families of octa-phase sequences of period  $(2^r-1)$  from  $\mathcal{K}$  families over  $Z_8$ .
3. Families derived from  $\mathcal{K}$  families over the local ring  $P_p^n[w^k]$ .

Table 1.3.1 Some Parameters of  $m$ -sequences over  $Z_2$  and  $Z_4$

Properties	$Z_2$	$Z_4$
Period	$(2^r-1)$	$(2^r-1)$
No of distinct cyclically equivalent sequences for a given generating element $\alpha$ .	1	$(2^r+1)$
Total number of sequences	$E(r)$	$(2^r-1)E(r)$

$$E(r) = \phi(2^r-1)/r; \phi(n) : \text{Euler's } \phi \text{ function.}$$

*Families of quadriphase sequences derived from  $\mathcal{K}$  families over  $\mathbb{Z}_4$ :* Quadriphase sequences are constructed from sequences over  $\mathbb{Z}_4$  through a quadriphase mapping given by  $\phi(a) = \omega^a$ , where  $\omega = \sqrt{-1}$ . Periodic correlation properties (correlation values and their distribution) of the quadriphase sequences are obtained in terms of their correlation transform distributions by using the properties of an Abelian association scheme on the elements of  $\text{GR}(4, r)$ . Two important families of quadriphase sequences derived from  $\mathcal{K}$  families over  $\mathbb{Z}_4$  are

(a) Families of quadriphase sequences of period  $(2^r - 1)$ ; each family consisting of  $(2^r + 1)$  sequences. The correlation transform distribution of these families is obtained by making use of the properties of an Abelian association scheme defined over  $\text{GR}(4, r)$ . The crosscorrelation values belong to the set

$$\begin{aligned} \{(-1), (\pm 2^t - 1 \pm j 2^t)\} & \quad \text{for } r \text{ odd, } r = 2t + 1; j = \sqrt{-1} \\ \{(-1), (\pm 2^t - 1), (-1 \pm j 2^t)\} & \quad \text{for } r \text{ even } r = 2t. \end{aligned}$$

Note that the modulus square of the correlation value,  $|\theta^2|$  is approximately equal to the length of the sequences. The  $\mathcal{K}$  family thus satisfies the Welch bound on  $\theta_{\max}$ . For each primitive  $\alpha$ , a family of  $m$ -sequences,  $\mathcal{K}^\alpha$  can be constructed. The number of cyclically equivalent families are shown to be equal to  $\phi(2^r - 1)/r$ , where  $\phi$  is the Euler's  $\phi$  function which is equal to the number of integers  $\leq 2^r - 1$  and relatively prime to  $2^r - 1$ .

(b) Families of quadriphase sequences of period  $2(2^r - 1)$ ; each family consisting of  $(2^{r-1} + 1)$  sequences: Any group of units  $\text{GR}^*(4, r)$  of a Galois ring  $\text{GR}(4, r)$  is a direct product of two groups  $G_a$  and  $G_c$ , where  $G_a$  is Abelian group of order  $2^r$ , and  $G_c$  is the cyclic component group of order  $2^r - 1$ . Associated with every element  $\gamma$  of  $G_a \in \text{GR}^*(4, r)$ ,  $\gamma \neq 1$ , a family of sequences of period  $2(2^r - 1)$  is defined as a family of trace sequences generated by  $\gamma\alpha$ , where  $\alpha$  is a primitive element of  $G_c$ . Thus for every  $\alpha$ , there are  $2^r - 1$  families. These sequences are shown to be interleaved  $m$ -sequences (im-sequences) of period  $2(2^r - 1)$ , and hence are called interleaved  $m$ -sequence families, in short  $\mathcal{IK}$  families. Let  $\gamma = 1 + 2\gamma' = 1 + 2\bar{\gamma}$ ; where  $\bar{\gamma} = \gamma' \bmod 2$ ,  $\gamma' \in G_c$ . Three families of  $m$ -sequences are identified depending on the specific nature of  $\gamma$ . These are

1. Families  $(\mathcal{IK}^{\bar{\gamma}})$ , with  $\text{trace}(\bar{\gamma}) = 1$
2. Families  $(\mathcal{IK}^{\bar{\gamma}})$ , with  $\text{trace}(\bar{\gamma}) = 0$ ,  $\gamma \neq 1$
3. A family  $(\mathcal{IK}^3)$

Correlation values of these sequences are computed from the correlation values of  $m$ -sequences. Among  $2^r - 1$  families,  $2^{r-1}$  families  $\mathcal{IK}^{\bar{\gamma}}$ ,  $\text{trace}(\bar{\gamma}) = 1$ , are optimal, and satisfy Welch's bound on  $\theta_{\max}$ . Rest of the  $2^{r-1} - 1$  families are suboptimal, wherein  $\theta_{\max}$  is approximately equal to  $\sqrt{2L}$ ;  $L = 2(2^r - 1)$ . The family



$\mathcal{M}^3$  is optimal only for the case when  $r$  is odd. The linear complexity of these sequences is same as that of  $m$ -sequences i.e.  $r$ . The new quadriphase families derived in this thesis are given in the Table 3.5.4.

Sole [31] was first to construct a family of  $(2^r+1)$   $m$ -sequences of period  $2^r-1$  over  $Z_4$ . He also determined the correlation properties for  $m$ -sequences with period  $2^r-1$  ( $r$ : an odd integer) by making use of an Abelian association scheme given by Liebler and Mena [40]. On the similar lines we have given a closed form correlation expression for even values of  $r$  [30]. Boztas and Kumar [32] have also given the same set of sequences. However, their proof of correlation values is based on the theory of exponential sums. Enumeration of correlation properties of  $m$ -sequences over field or ring using association schemes is a novel concept and very interesting.

While preparing the thesis, we became aware of a paper by Boztas, Hammons, Kumar [33] which contains extension of their earlier results on  $m$ -sequences in [32]. The paper [33] describes two families; Family A and Family B. These families correspond, in our classification, to  $m$ -sequence family and an  $Im$ -sequence family  $\mathcal{M}^{\gamma}(\text{tr}(\tilde{\gamma}) = 1)$ . The families  $\mathcal{M}^{\gamma}(\text{tr}(\tilde{\gamma}) = 0)$  and  $\mathcal{M}^{\gamma}(\gamma=3)$  are additional sub-families among  $\mathcal{M}$ -sequence family of period  $2(2^r-1)$ . Moreover, the approach taken in this thesis is mainly based on the association schemes on  $GR(4,r)$  and the properties of  $GR(4,r)$ ; whereas in [33], the theory of exponential sums is used for computing correlations. The Galois ring framework used in the thesis takes care of all the results in [33] and appears to be more general than the one used in [33].

*Families of octaphase sequences of period  $(2^r-1)$  from  $\mathcal{M}$  families over  $Z_8$ :* For any primitive element  $\alpha$ , family of  $m$ -sequences over  $Z_8$  consists of  $(4^r+2^r+1)$  sequences of period  $2^r-1$ , which includes sequences over ideals  $\langle 2 \rangle$  and  $\langle 4 \rangle$ . Excluding the sequences over ideals  $\langle 2 \rangle$  and  $\langle 4 \rangle$ , there are  $4^r$  proper sequences over  $Z_8$ . These  $4^r$  proper sequences are divided into  $2^r$  sets each consisting of  $2^r$   $m$ -sequences which can be used for 8-PSK modulated CDMA communication systems. These sets satisfy what Massey has described as code sets satisfying Welch bound with equality [41] (Not Welch bound on  $\theta_{\max}$ ). This implies that  $\theta_{\text{rms}}$ , the root mean square of the inner-product values between all pairs of various time shifted versions of sequences in a family  $F$  (expression for  $\theta_{\text{rms}}$  given below), is approximately equal to  $\sqrt{L}$ ,  $L$  being the period of the sequences, and this is the smallest value possible.

$$\theta_{\text{rms}} = \frac{1}{M(ML-1)} \left( \sum_{\substack{X \in F \\ \text{except } X=Y}} \sum_{\substack{Y \in F \\ \& \tau \neq 0}} \sum_{\tau=0}^{L-1} |C_{XY}(\tau)|^2 \right),$$

where  $M$  is the number of sequences in  $F$ . This is precisely the appropriate requirement for CDMA operations where many users are operating in the system.

*Families derived from  $\mathcal{K}$  sequences over the local ring  $P_p^n[w^k]$ :* Sequences over  $P_p^n[w^k]$  are used to derive frequency hopping patterns and sequences with good block inner-product correlations. Note that  $P_p^n[w^k]$  is a matched structure for both block inner-product and Hamming correlations. The frequency hopping patterns are obtained by associating with each symbol  $a$  in the ring  $P_p^n[w^k]$ , a distinct frequency  $f_a$  belonging to the frequency library. For efficient operation, it is required that mutual Hamming correlation between any two hopping patterns within a family should be small. A family of sequences over  $P_p^n[w^k]$ , denoted by  $\mathcal{K}(A)$ , is constructed, corresponding to each  $m$ -sequence  $S^A$ ,  $A \in \text{PGR}(V^k, r)$ . The number of sequences in  $\mathcal{K}(A)$  is determined by the number of distinct elements of  $P_p^n[w^k]$  occurring in  $S^A$ .

By making use of  $\mathcal{K}(A)$  families, where  $A \in \text{PGR}(V^k, r)$  and  $V$  is the order of the residue field,  $V^{r-\rho}$ ,  $0 \leq \rho \leq k$ , coincidence frequency patterns of size  $V^\rho$  and period  $V^r-1$  are constructed. These frequency patterns meet Lempel and Greenberger bound on  $H_{\max}$  [2], which is the maximum of out of phase autocorrelation values and crosscorrelation values between any two hopping patterns. The derived frequency patterns include familiar one-coincidence frequency patterns.

Families derived includes familiar one coincidence sequences also. Shaar et al. [42] have presented general description of a class of one-coincidence sequence sets by using  $n$  linearly independent phases of binary  $m$ -sequences. This class of one-coincidence sequences can be obtained from the frequency hopping families derived from  $P_2^n[w^k]$ . Recently J.J. Komo and S.C. Liu [43] have described frequency hopping patterns from  $m$ -sequences over  $\text{GF}(2^r)$ . In [43], authors make note of a sequence over  $\text{GF}(2^2)$ , which is constructed by grouping two binary  $m$ -sequences, sharing many properties of  $m$ -sequences and yet not an  $m$ -sequence over  $\text{GF}(2^2)$ . It is indeed an  $m$ -sequence over  $P_2^2[w^2]$  and rightly not an  $m$ -sequence over  $\text{GF}(2^2)$ . Our approach characterizes all such obtainable sequences by appropriately grouping  $m$ -sequences over finite fields. The weight distribution of  $m$ -sequences over  $P_p^n[w^k]$  is also given.

In addition to above results, we also derive a subset of  $m$ -sequences over  $P_p^n[w^k]$  having only two level block inner-product autocorrelation; out of phase autocorrelation value being  $-n$ .

*I(b) Non-linear Constructions (Sequences with Controllable Linear Complexity):* The families of sequences derived under this heading are nonlinear in the sense that the sequences in a family are not

closed under pointwise addition. The linear complexity (LC) of a sequence is the shortest length linear feedback shift register which generates the sequence. Even though nonlinear property hinders the evaluation of correlation parameters, sequences possessing this property are essential in certain environments. In spread spectrum communication systems, apart from the good correlation properties it is desirable to have sequences with large LC. The  $r$  length linear recursion of a sequence over a field can be solved by using  $2r$  consecutive sequence bits, by using Berlekamp–Massey algorithm [44]. Similar algorithm for sequences over  $Z_M$  exists due to Reed and Sloane [45]. The same algorithm is extendible to sequences over  $P_p^n[w^k]$  also. Thus if the LC of the code sequence used for communications is small then this helps an intelligent jammer to duplicate the sequence generation mechanism by observing the finite segment of the sequence. Hence a robust system would employ sequences with large LC.

Evaluation of LC of finite field sequences is greatly facilitated by using Blahut's theorem which says that the LC of a sequence is equal to the number of non-zero terms in the discrete Fourier transform representation of the sequence [46]. An extension of Blahut's theorem for the case of sequences over rings is stated and has been made use of for the computation of LC of sequences over finite rings.

The important results obtained are classified into the following two categories.

1. Generalized Polynomial Sequences
2. Sequences Obtained From Mappings from a Ring to its Ideals

*Generalized Polynomial Sequences:* A generalization of a complexity enhancement procedure for field  $m$ -sequences [47] to sequences over residue rings is presented. This is an extension of polynomial sequences of field case. The scheme makes use of generalized permutation polynomials over Galois extension ring. The method for complexity enhancement of trace sequences over residue class rings is illustrated below.

Let  $\mathcal{R}$  be a residue class local ring ( $Z_4$  or  $P_p^n[w]$ ). Let  $GR(\mathcal{R}, r)$  be  $r^{\text{th}}$  degree Galois extension ring.

- 1: Consider a maximum length sequence  $\{y_i\}$  over extension ring  $GR(\mathcal{R}, r)$  with  $u$  linear span.
- 2: Using a suitable permutation on  $GR(\mathcal{R}, r)$ ,  $y_i$ 's are permuted.

$$y_i' = \text{permutation}(y_i), y_i \in \{y_i\}$$

- 3: The sequence  $\{s_i\}$  is then defined as the trace function of  $\{y_i'\}$

$$s_i = \text{tr}_1^r(y_i')$$

- 4: The resulting sequence  $\{s_i\}$  over  $\mathcal{R}$  has large LC.

A corresponding complexity enhancement scheme for field  $m$ -sequences [47], with permutation monomials as permutation in step 2, results in GMW sequences [48]. Two generalizations of permutation monomials over  $GR(4,r)$  are obtained from permutation monomials over  $GF(2^r)$ . These have been used in the above scheme and consequently two families of generalized GMW (GGMW) sequences over  $Z_4$  of period  $2^{ru}-1$  are defined, where  $u$  is a positive integer. The size of the GGMW family is  $2^{ru}+1$  and the  $\langle 2 \rangle$  ideal sequence is isomorphic to a binary GMW sequence.

The LC of GGMW sequences is computed and shown to be in the range.

$$\{r(u^{H(b)}), \dots, r(u^{H(b)}) - \frac{(2^{ru}-1)}{(2^r-1)} r\} \quad (1.3.1)$$

where  $H(b)$  is the number of ones present in the binary representation of  $b$ , a integer in the range  $0 \leq b \leq 2^r-1$ . Correlation properties these families satisfy Welch bound on inner product with equality, which implies that the  $\theta_{rms}$  is approximately equal to  $\sqrt{L}$ ,  $L$ :period. However,  $\theta_{max}$  deviates from optimal value of  $\sqrt{L}$ ; computer results suggest that frequency of deviation is not large.

A similar procedure for LC enhancement for sequences over  $P_p^n[w^k]$  is also considered and a family of GGMW sequences of period  $V^{ru}-1$  is introduced. By using a subset of GGMW sequences, families of optimal frequency hopping sequences are constructed. The LC of a GGMW sequence is show to be equal to that of its residue sequence over  $P_p^m[w]$ . When  $p=2$ , it is shown that the LC of the GGMW sequences over  $P_2^n[w^k]$  is equal to  $r(u^{H(b)})$ , where  $H(b)$  is as defined in (1.3.1). The families satisfy Lempel and Greenberger bound on  $H_{max}$ . The generalized polynomial sequences satisfy a generalized  $r$ -tuple distribution.

*Sequences Obtained From Mappings from a Ring to its Ideals:* Sometimes, mappings from a ring to its ideals yield useful families of sequences. An example of such mappings is the familiar homomorphic mappings from local rings to its ideals. But, these mappings produce structurally similar sequences and hence of not much import. We consider a nonlinear polynomial ( $\mathcal{NLP}$ ) mapping from  $Z_4$  to its ideal  $\langle 2 \rangle$ , given by  $\varphi(x) = x^2 - x$ . This mapping results in sequences over the ideal  $\langle 2 \rangle$  which are structurally different from the sequences over  $Z_4$ . The ideal  $\langle 2 \rangle$  is isomorphic to the binary field and the quadriphase mapping  $\phi$  (Refer (1.2.4)) on the ideal results in bi-phase signal set. Thus biphas sequences are constructed from sequences over  $Z_4$ . The quadriphase families derived in this thesis are considered for biphas sequence design. The families of biphas sequences thus derived from families of  $Z_4$  sequences are

denoted by prefixing a word ' $\mathcal{NLP}$ ' to their corresponding  $Z_4$  family name. Following two families of biphasic sequences are derived from  $Z_4$  families.

1. Families of biphasic sequences ( $\mathcal{NLP}\mathcal{M}$ ) of period  $(2^r-1)$  from ( $\mathcal{M}$ ) families over  $Z_4$ ; each family consisting of  $(2^r+1)$  sequences.
2. Families of biphasic sequences of period  $2(2^r-1)$  ( $\mathcal{NLP}\mathcal{IM}$ ) derived from  $\mathcal{IM}$  families over  $Z_4$ ; each family consisting of  $2^{r-1}+1$  sequences.

The  $\mathcal{NLP}$  mapping considered is similar to the quadriphase to biphasic transformation given in [3]. Also in [3], a method of evaluating correlation properties of transformed sequences is given and a bound on  $\theta_{\max}$  is provided;  $\theta_{\max}^B \leq 2^* \theta_{\max}^Q$ , where superscripts B and Q indicates for binary and quadriphase sequences. The same correlation evaluation technique is used here also. But, crosscorrelation distributions of biphasic families are computed using the properties of GR(4,r) and correlation transform distributions of the corresponding  $Z_4$  families. Many biphasic families are shown to satisfy Sidelnikov ( $\theta_{\max} \leq \sqrt{2L}$ ) and Welch bounds ( $\theta_{\max} \leq \sqrt{L}$ ) on  $\theta_{\max}$ .

Another interesting feature of biphasic sequences given here is their large LC property; it follows from the nonlinear nature of polynomial function considered. The generalized Blahut's theorem on  $Z_4$  is used to compute LC of resultant binary sequences. The LC of sequences in  $\mathcal{NLP}\mathcal{M}$  family is lower bounded by  $r(r-1)/2$  and the LC of sequences in  $\mathcal{NLP}\mathcal{IM}$  families is shown to be equal to  $r(r+3)/2$ . The new biphasic families derived from  $Z_4$  families are given in Table 6.6.1 along with their correlation and LC properties.

## II. Families Derived from the Representation of Semi-local Rings

Families derived under this heading are useful in slow frequency hopping spread spectrum (SFHSS) systems. In SFHSS systems, one or more symbols are transmitted within one frequency hop (slot) and a hit would mean total loss of data transmitted in that hop. Thus, apart from minimizing the mutual Hamming correlation between patterns, hits resulting from presence of all the sequences in the system should be minimized. This implies that sequences should have good generalized Hamming correlation properties (Eqs (1.2.5) & (1.2.6)). By utilizing properties of orthogonal ideals of polynomial residue class ring, and families derived over local rings, we construct families of sequences over semi-local rings having ideal GHCC (crosscorrelation function is equal to zero for all values of  $\tau_i$ ). The construction is mainly based on the internal direct sum representation of the ring  $P_p^n[W(\xi)]$ . Following new families are derived.

1. A family of  $p^{n_2}$  sequences of period  $L = p^{n_1-1}$  over  $P_p^n[w(\xi)]$ , where  $n = n_1 + n_2$ , by using a sequence over  $P_p^{n_1}[w_1(\xi)]$  of period  $p^{n_1-1}$ , where  $w_1(\xi)$  is an irreducible factor (of degree  $n_1$ ) of  $w(\xi)$ . These sequences satisfy ideal GHCC properties.
2. A family of  $\mu p^{n_2}$  sequences of period  $L = p^{n_1-1}$  over  $P_p^n[w]$ ,  $n = n_1 + n_2$ , by using  $\mu$  one-coincidence sequences over  $P_p^{n_1}[w_1(\xi)]$  each of period  $p^{n_1-1}$ . The GHCC and GHAC for any sequence in the family are given by

$$\begin{aligned} \text{GHAC}_m(\tau_1, \tau_2, \dots, \tau_{m-1}, \tau_{m+1}, \dots, \tau_n) &\leq p^{n_1-1} \mu \text{ for } \tau_j = 0 \\ &\leq \mu - 1 \text{ otherwise.} \end{aligned}$$

$$\text{GHCC}_m(\tau_1, \tau_2, \dots, \tau_n) \leq \mu - 1 \text{ for all } \tau_i \neq \tau_j.$$

A code generation scheme, based on the direct sum decomposition of semi-local rings, for slow hopping multiple access communication systems is given where different users can have different frequency diversity.

## 1.4 Literature Survey.

Literature on construction of sequences with desired correlation and related properties is vast and there are excellent texts and survey articles available on this topic [1,4,5,19,23]. Our idea is not to review the entire set of results in this area. Works are quoted in accordance with the perspective taken in the thesis. Mainly constructions of sequences using algebraic approach have been considered for the survey. An approach which uses geometric results has also resulted in quite good constructions [49–51]; some of them can also be defined in algebraic framework [48]. We do not attempt to review results concerning the heuristic search approach for construction of sequences, which deals mainly with sequences having good autocorrelation properties [15–18]. Some results of this category which are found using computers are available in articles in the journal 'Electronic Letters' [52,53].

The review attempts to give a general idea of the development in the area of algebraic construction of sequences. It is organized according to correlation and other relevant properties of sequences. Most of the results on algebraic construction of sequences are concerned with polyphase sequences with good inner-product correlations. Important structural methods, like generation of sequences using linear feedback shift register (LFSR) and generation of sequences using trace functions, were first obtained while searching for sequences with good inner-product correlations.

1. *Inner-product correlations*: Constructions of pseudo-noise (PN) sequences (using LFSRs) having good inner-product correlation properties provide the earliest examples of the structural approach in the literature. The study of PN sequences started somewhere in mid fifties. Some of the early pioneers in this area are Golomb and Zierler [5,54]. Major results of Golomb's study during fifties and sixties are found in his book [19], published in 1967. The theory of linear recursions which Golomb and Zierler used to construct PN sequences was known in the mathematical literature much earlier [55,56]. However, its influence on communication engineers was little [5]. Initial work of Huffman [57] deals mainly with implementation aspects of feedback shift registers.

Trace function representation was introduced in sequence studies somewhere in the later half of sixties by many authors [23,58–60]. This played a key role in the development of the subject due to its elegant representation and its usefulness in evaluation of sequence properties. In the context of use of trace function in the development of sequence theory, two phases can be identified in the literature:

Phase I (sixties): when trace functions are employed mainly as a tool to compute crosscorrelations of binary  $m$ -sequences.

Phase II (eighties): when trace functions are used as effective tool to obtain new constructions.

Computation of crosscorrelation parameters of  $m$ -sequences and Gold sequences invariably requires properties of trace functions [21,23,58]. While autocorrelation results can be proved even without trace representation, crosscorrelation computations are impossible without this tool [23]. Even while trace functions were indispensable tools for correlation computation during sixties and seventies, shift register representation of sequences was mainly followed for their implementation. It was only in eighties that these were effectively used to get new constructions. Probably, first result in this series is by Olsen et. al. [61] on Bent function sequences. A paper by Scholtz and Welch [48], giving algebraic description of GMW sequences, effectively exploits the power of trace functions. No sequences [62], Kumar and Moreno sequences [63], Liu and Komo sequences [64], polyphase sequences by Moriuchi and Imamura [65], Cascaded GMW sequences by Klaper et. al. [66] are some of recent examples which make use of trace function representation.

The constructions mentioned above are all defined over finite fields, properties and structure of which are quite well known among researchers in the area of sequence constructions; there are many excellent texts dealing with properties of finite fields [24,67,68]. Contrary to it, structure and properties of finite rings are not familiar to researchers in this area. To author's best knowledge, Scholtz and Welch [69]

in 1978 were first to consider the ring  $Z_M$  for sequence design. They have reported sets of sequences with good aperiodic and periodic inner-product correlation properties derived from group characters of  $Z_M$  through a computer assisted study. Next is a paper by Sole [31] which gives a construction of a family of  $(2^r+1)$   $m$ -sequences over  $Z_4$  of period  $2^r-1$  and their correlation properties ( $r$ : an odd integer) by making use of an Abelian association scheme given by Liebler and Mena [40]. On the similar lines we have given a closed form correlation expression for even values of  $r$  [30]. Recently Boztas, Hammons and Kumar [33] have reported same set of sequences. In both [30] and [33], trace functions over Galois rings have been employed for sequence construction. However, proof of correlation values in [33] is based on the theory of exponential sums and trace functions. We have followed an approach for correlation computation based on an Association scheme defined on the elements of the Galois ring  $GR(4,r)$  [29,30].

There are various bounds on the inner-product correlation values for polyphase sequences [34,35,70–72]. Important among them are Welch bound [34], Sidelnikov bound [35] on  $\theta_{\max}$ . The earliest paper dealing with a bound on  $\theta_{\max}$  for binary sequences is by Stalder and Cahn [71]. Recently Massey [41] has rederived Welch bound and has given a necessary and sufficient condition for signal sets satisfying Welch bound with equality. This paper gives a bound on  $\theta_{\text{rms}}$ , which is equal to the root-mean-square of the inner product values between all pairs of various time shifted version of sequences in a family.

**2 Hamming Correlation:** Costas sequences are the earliest discovery of sequences with good Hamming correlation properties [73]. But, they were found with coincidence property as a criterion rather than Hamming correlation. Lempel and Greenberger [2] were first to consider Hamming correlations as criteria for construction of sequences. They have given lower bounds on Hamming correlations of sequences for a given length and alphabet size which is tight. They have also described optimal families derived from  $m$ -sequences over  $GF(p)$ . This paper is most influential and referred to by most of subsequent researchers in this area. Another important linear construction considered is derived from Reed–Solomon codes [5,74,75]. Kumar [76] has derived frequency patterns from Bent functions and Bent function sequences having good linear complexity. This is a nonlinear design and Hamming correlation properties are near optimal.

**3 Block Inner-product Correlation:** Block Inner-product correlation function is considered by Komo [77], Park and Komo [78,79] for CDMA which uses block PSK modulation, a generalization of PSK modulation. But we are not aware of this kind of modulation being used in practice. In [43], authors use this correlation to analyze frequency hopping patterns.



4 *Lee correlations:* We have not come across any reference which deals with this kind of correlation function. But, this might have application in phase modulated systems as lee metric is suited to phase modulated channels [39,80].

5 *Controllable Linear Complexity (LC) :* A paper by Groth [81] deals with generation of binary sequences with controllable LC by linear generator with nonlinear feed-forward function. Key [82] gives upper bound on LC attainable by nonlinear feed-forward generators. The articles in Advances in Cryptology and Applied Algebra and Error Correcting Codes (AAECC) conferences (Published in Lectures notes in Computer Science Series, Springer Verlag) contain large number of papers dealing with this subject; most of them deal with applications in cryptography. The applications in secure communication systems demand sequences with good correlation properties along with large LC. Nonlinear sequences with good correlation properties are scarce. The bent sequence construction [61] is one of the elegant method of obtaining binary sequences with good LC and correlation properties. Kumar's paper [76] makes use of bent functions and bent sequences to derive finite field sequences with good LC for frequency hopping. Papers by Brynielsson [83] and Siegenthaler and Forre [47] give algebraic methods of obtaining sequences with controllable LC with good correlation properties. They show how GMW sequences can be obtained as a special case of their method. Recent generalizations of GMW sequences are given in [66,84].

There are hardly any references dealing with sequences over rings with controllable complexity [30]. However recently, rings have been used to construct binary sequences with large LC [85].

6 *Multiplexing applications:* The earliest reference which makes use of ring structure for multiplexing operation is that of Murakamin et. al.[86]. They have used the decomposition of a semi-simple ring as a direct sum of Galois fields for efficient coding scheme in a multichannel communication system. Nishikado et.al. [26] have proposed a encoding and decoding scheme by making use of cyclic codes over finite fields. This scheme has a feature of error correction when message rate is lower than the regular speed. The generalized version of this scheme is described in [25].

## 1.5 Organization of the Thesis

Chapter 2 discusses correlation and other related properties in connection with the sequences over residue class rings and establishes necessary tools for evaluation of various correlation functions required for the entire thesis. In Section 2.1, a generalized correlation function between a pair of sequences is defined such that specific correlation functions can be derived as special cases. Expressions for correlation

transform of sequences over  $Z_2$ ,  $Z_4$  and  $Z_8$  are also given. In Section 2.2, several examples of residue class rings are identified which are matched to different signal sets for various correlation functions. Equivalences of some of the correlations functions are treated in Section 2.3. It is shown that binary block inner-product correlations are equivalent to binary block Hamming correlations. Generalized Hamming correlation functions which depend on all the sequences employed in the system are given in Section 2.4. Section 2.5 discusses some of the criteria for correlation and other parameters often considered in practice. Conditions for sequence sets satisfying Welch bound with equality are given. A generalized version of Blahut's complexity theorem applicable to sequences over residue class rings is also given. This has been used to compute the LC of sequences constructed in the thesis.

Chapter 3 is concerned with generation of sequences over  $Z_4$  and  $Z_8$  and their applications in constructing quadriphase and octaphase sequences. Essential mathematical background required for the chapter is given in Section 3.1 and 3.2. Properties of Galois extension ring of  $Z_4$  of degree  $r$ , denoted as  $GR(4,r)$ , needed for the paper, are briefly reviewed in Section 3.1. Relevant properties of an algebraic Abelian association scheme defined on the elements of  $GR(4,r)$  are given in Section 3.2. Families of trace function sequences are defined in Section 3.3. Trace functions (given in Appendix A) over  $GR(4,r)$  and the Abelian association scheme are used extensively in Sections 3.4 and 3.5 to define various families of quadriphase sequences and to obtain their correlation properties. Section 3.4 presents a family of  $L+2$  maximal length sequences ( $m$ -sequences) over  $Z_4$  of period  $L = 2^r - 1$ . The Abelian association scheme on the elements of  $GR(4,r)$  has been used to calculate crosscorrelation and out-of-phase autocorrelation values of sequences. Section 3.5 deals with the construction of sequences with period  $2(2^r - 1)$ . The correlations are computed from the analytical correlation expressions of  $m$ -sequences. Maximal length sequences over  $Z_8$  which can be used in octaphase communication systems are discussed in Section 3.6. Subsets of maximal length sequences over  $Z_8$  are identified which satisfy Welch bound with equality.

Chapter 4 discusses generation and properties of maximal length sequences over  $P_p^n[w^k]$  and their applications in constructing frequency hopping patterns and sequences with good block inner-product autocorrelations. Section 4.1 gives vector space structure of  $P_p^n[w^k]$  and  $PGR(V^k, r)$  and their relevant properties. Section 4.2 defines families of trace sequences over  $P_p^n[w^k]$ . Definition and properties of maximal length sequences over  $P_p^n[w^k]$  are discussed in Section 4.3 and 4.4. Families of frequency hopping patterns derived from  $m$ -sequences are given in Section 4.5. Constructions of sequences with ideal block inner-product correlations are given Section 4.6.

Chapter 5 gives construction and properties of controllable large LC sequences over residue class rings  $Z_4$  and  $P_p^n[w^k]$ . The sequences over  $Z_4$  and  $P_p^n[w^k]$  are respectively employed to get quadriphase sequences and frequency hopping patterns. Section 5.1 gives generalized permutation monomials over  $GR(4, r)$  and  $PGR(V^k, r)$ . Section 5.2 discusses a generalized procedure for constructing large LC sequences obtained from trace sequences using permutations on Galois extension rings. Families of GGMW sequences over  $Z_4$  and  $P_p^n[w^k]$  are defined in Section 5.3 using permutation monomials over appropriate Galois extension rings. Sections 5.4 and 5.5 give properties of GGMW sequences over  $Z_4$  and  $P_p^n[w^k]$  respectively.

Chapter 6 gives a construction of sequences over the proper ideal of  $Z_4$ ,  $< 2 >$ , with controllable LC using families of  $Z_4$  sequences. The construction makes use non-linear polynomial mappings from  $Z_4$  to  $< 2 >$  and the quadriphase mapping  $\phi((1.2.4))$ . Section 6.1 gives nonlinear polynomial mappings from  $Z_4$  to  $< 2 >$ . Section 6.2 gives correlation expressions for biphasic sequences in terms of correlation values of its corresponding  $Z_4$  sequences. Sections 6.3 and 6.4 discuss definition and properties of families of biphasic sequences derived from  $\mathcal{M}$  and  $\mathcal{NM}$  families of  $Z_4$  sequences respectively. LC of the sequences are computed in Section 6.5. Comparison of new families of biphasic designs with known families is given in Section 6.6.

Chapter 7 deals with construction of slow frequency hopping (SFH) patterns derived from sequences over semi-local ring  $P_p^n[w(\xi)]$ . These sequences are of importance in SFH multiple access communication systems. Section 7.1 gives a brief description of SFH multiple access communication systems and requirements on the hopping patterns. Section 7.2 gives a construction of SFH patterns with ideal generalized Hamming correlation properties. The construction makes use of decomposition of  $P_p^n[w(\xi)]$  into direct sum of its orthogonal ideals. Construction of SFH patterns derived from one-coincidence sequences over  $P_p^{n_1}[(w_1(\xi))^k]$ , where  $n_1 < n$  and  $w_1(\xi)$  is a factor of  $w(\xi)$ , is given in Section 7.3. Section 7.4 gives a SFH pattern generation procedure where different users have different frequency expansion factors.

Appendix A gives relevant algebraic results concerning ring  $Z_{2^k}$  and its Galois extension ring  $GR(2^k, r)$ ,  $k$  being a positive integer, which are necessary for the entire thesis. Appendix B gives proofs of properties of automorphisms and trace functions defined over  $GR(2^k, r)$ . Some irreducible polynomials over  $Z_4$  and  $Z_8$  are given in Appendix C. Appendix D gives relevant properties of ring  $P_p^n[w^k]$  and its Galois extension ring  $PGR(V^k, r)$ . Appendix E gives a Massey's conditions [41] for sequence sets satisfying Welch bound with equality. Internal direct sum representation of semi-local ring  $P_p^n[w(\xi)]$ , where  $w(\xi)$  is a composite polynomial over  $GF(p)$  of degree  $n$ , is given in Appendix F.

## Chapter 2

### Correlation and Related Properties of Sequences over Residue Class Integer and Polynomial rings

This chapter discusses correlation and other related properties in connection with the sequences over residue class rings and establishes necessary tools for evaluation of various correlation functions as required in the thesis. A generalized correlation function between a pair of sequences is defined such that specific correlation functions of practical importance can be derived as special cases. Notion of finite ring sequence alphabet matched to signal set for a correlation function introduced in Section 1.2 is further discussed. Several examples of residue class rings are identified which are matched to different signal sets for various correlation functions.

Equivalences of some of the correlations functions are also given in this chapter. Two correlation functions are equivalent if the computation of correlation values from one type is sufficient to determine the correlation values from the equivalent correlation function. This equivalence leads to efficient implementation of some synchronization schemes.

Generalized Hamming correlation functions which depend on all the sequences employed in the system are given. They are useful in slow frequency hopping spread spectrum communications.

Correlation functions are the properties of sequences. However, the communication system requirements impose restrictions on their values for proper system operation. Some of the criteria for parameters often considered in practice are discussed. Apart from the correlation properties, sequences should possess large linear complexity (LC) for communication systems where jamming by unintentional users is a major threat [5,61]. Blahut's theorem on LC is used for computation of LC of periodic sequences over finite field of period which are DFT transformable (period should divide  $p^r - 1$ ;  $r$  is a positive integer and  $p$  is the characteristic of the field) [46]. A generalized version of this theorem applicable to sequences over residue class rings is given; it constitutes the main tool for evaluation of LC of ring sequences derived in this thesis.

## 2.1 Generalized Correlation Function

As a means of quantifying the distinguishability of sequences, several types of autocorrelation and crosscorrelation functions have been used in practice. The type of correlation function used mainly depends upon the application where the sequences are used, the modulation, and the type of channel. In the communication context, the correlation properties are critical mainly in

- a) Synchronization of transmitter and receiver amongst different users in the system.
- b) Sharing the common communication bandwidth for multi-user operation.

In applications where only single user is operating in the system, such as in radar systems, ranging systems, spread spectrum, scramblers, autocorrelation function is important. Both autocorrelation and crosscorrelation properties are important in multi-user applications such as CDMA systems, spread spectrum multiple access systems, simultaneous ranging to several systems. Sequences used in most of the applications are periodic due to their implementational simplicity. Two important correlation functions commonly used are periodic and aperiodic correlation functions. For sequences over complex numbers they are defined as follows. The periodic crosscorrelation function  $PC_{AB}(\tau)$  between two complex sequences A and B of period L is given by

$$PC_{AB}(\tau) = \sum_{i=0}^{L-1} a_i b_{(i+\tau) \bmod L}^*$$

where \* denotes complex conjugation. The aperiodic crosscorrelation function  $APC_{AB}(\tau)$  between two complex sequences A and B of period L is given by

$$\begin{aligned} APC_{AB}(\tau) &= \sum_{i=0}^{L-1-\tau} a_i b_{i+\tau}^*, \text{ if } 0 \leq \tau \leq L-1 \\ &= \sum_{i=0}^{L-1+\tau} a_{\tau-i} b_i^*, \text{ if } 1-L \leq \tau < 0 \\ &= 0 \text{ if } |\tau| \geq L \end{aligned}$$

Two important correlation functions are derived from aperiodic correlation function; they are even and odd correlation functions,  $C_{AB}(\tau)$  and  $\hat{C}_{AB}(\tau)$ . They are given by

$$\begin{aligned} C_{AB}(\tau) &= AC_{AB}(\tau) + AC_{AB}(\tau-L) \\ \hat{C}_{AB}(\tau) &= AC_{AB}(\tau) - AC_{AB}(\tau-L) \end{aligned}$$

Even correlation function is the familiar periodic correlation function. Aperiodic and odd correlation functions are of importance in many applications. However, they are hard to compute and many times they are determined using a computer. Whereas, periodic correlation functions are analytically more

tractable and are dealt with extensively in the literature. In this thesis also only periodic crosscorrelations are considered.

To take care of various correlation functions of practical importance, a generalized correlation function between a pair of sequences is defined. A close examination of these correlation functions reveals that definitions of correlation functions involve some distance measures in the space of signals. The effort here is to present the correlation functions in a generalized setting where various correlation functions can be derived as special cases with different distance measure definitions. The definition of periodic correlation is assumed throughout, which means that indices in the sequence are always taken modulo  $L$ ;  $L$  being the sequence period.

**Definition 2.1.1:** Let  $A = \{a_0, a_1, \dots, a_{N-1}\}$ ,  $B = \{b_0, b_1, \dots, b_{N-1}\}$  be two sequences of period  $L$  over certain alphabet  $\mathcal{A}$  of size  $|\mathcal{A}|$ . Then crosscorrelation function  $C_{AB}(\tau)$  between two sequences  $A$  and  $B$  is defined as

$$C_{AB}(\tau) = \sum_{i=0}^{L-1} f\{\phi(a_i), \phi(b_{(i+\tau) \bmod L})\}; \quad \tau = 0, 1, \dots, L-1 \quad (2.1.1)$$

where  $\phi$  is a mapping from the finite alphabet  $\mathcal{A}$  to an appropriate signal set which is a subset of real (complex) space, and  $f$  is a binary operation related to the definition of the correlation function which depends on the distance measure. The range of  $f$  is also a subset of real (complex) space. The nature of  $\phi$  and  $f$  depends on the modulation and the type of application where the sequences are used. The mapping  $\phi$  which links a finite ring and a signal set may be considered as an abstract modulator. Another function which helps in the computation of correlations is defined. It is called correlation transform.

**Definition 2.1.2:** The correlation transform of a sequences  $A$  is defined as the inphase correlation of  $A$  and the sequence which has all zero entries. It is given by

$$\kappa^{(f, \phi)}(A) = C_{AS^0}(0) = \sum_{i=0}^{L-1} f\{\phi(a_i), \phi(0)\}; \quad (2.1.2)$$

where  $S^0$  is the sequence with all zero entry. Superscript  $(f, \phi)$  in correlation transform notation may be dropped whenever the type of correlation  $(f, \phi)$  is clear from the context. In the following we list  $f$  and  $\phi$  for some of the more commonly used correlation functions.

1. *Inner-Product (IP) correlation*: In this case,  $\phi$  is a mapping from a finite structure  $\mathcal{A}$  to the set of  $M^{\text{th}}$  roots of unity, whose elements belonging to the complex field, given by

$$\phi(a) = \exp\left(\frac{\omega 2 \pi \phi'(a)}{M}\right), \omega = \sqrt{-1}; \quad (2.1.3)$$

where  $\phi'$  is a mapping from  $\mathcal{A}$  to  $Z_M$ . The binary operation  $f$  is a conjugate product operation given by  $f(a, b) = ab^*$ . Here the measure of distinguishability is the euclidean distance. The distance between a sequence  $A$  and any  $\tau^{\text{th}}$  shift of sequence  $B$  is given by

$$\sum_{i=0}^{L-1} [\phi(a_i) \pm \phi(b_{i+\tau})^*]^2 = \sum_{i=0}^{L-1} [\phi(a_i)^2 \pm \phi(b_{i+\tau})^{*2}] + 2 C_{AB}(\tau).$$

Thus for a fixed signal energy, it is easy to distinguish  $A$  from  $\tau^{\text{th}}$  shift of  $B$ , if and only if the magnitude of  $C_{AB}(\tau)$  is small.

This type of correlation is mostly used in environments where the phase shift keying is the modulation technique. Three important commonly used correlation functions viz. binary, quaternary and octary inner-product correlation functions are special cases of this type. In the binary case,  $\phi$  is a mapping from a finite alphabet  $\mathcal{A}$  to the biphase signal set  $\{1, -1\}$ , given by

$$\phi(a) = (-1)^{\phi'(a)} \quad (2.1.4)$$

where  $\phi' : \mathcal{A} \rightarrow \text{GF}(2)$ , a mapping from  $\mathcal{A}$  to  $Z_2$ ,  $f$  is a product operation in reals. In the quaternary case,  $\phi$  is a mapping from a finite alphabet  $\mathcal{A}$  to the set of  $4^{\text{th}}$  root of unity,  $\{1, -1, j, -j\}$ , given by

$$\phi(a) = \omega^{\phi'(a)}, \omega = \sqrt{-1} \quad (2.1.5)$$

where  $\phi'$  is mapping from  $\mathcal{A}$  to  $Z_4$ . In the octary case,  $\phi$  is a mapping from  $\mathcal{A}$  to  $8^{\text{th}}$  roots of unity, given by

$$\phi(a) = \exp\left(\frac{\omega 2 \pi}{8} \phi'(a)\right), \quad (2.1.6)$$

where  $\phi'$  is a mapping from  $\mathcal{A}$  to  $Z_8$ .

In the following we consider specifically sequences over  $Z_M$ . Here we give correlation transform expressions for IP correlations. These are used in subsequent chapters for correlation computation. Let  $A$  be a sequence over  $Z_M$ . Then correlation transform for IP correlations is given by

$$R(A) = \sum_{i=0}^{N-1} (\epsilon)^{a_i} \quad (2.1.7)$$

where  $\epsilon$  is  $M^{\text{th}}$  root of unity. Let  $W^A$  be the weight vector associated with a sequence  $A$ , with  $W_i^A$  being the number of symbols  $i$  in  $A$ . For  $M = 2, 4, 8$ ,  $R(A)$  expression given in (2.1.7) becomes

$$\Re(A) = (w_0^A - w_1^A) \text{ when } A \text{ is over } Z_2. \quad (2.1.8)$$

$$\Re(A) = (w_0^A - w_2^A) + \sqrt{-1} (w_1^A - w_3^A) \text{ when } A \text{ is over } Z_4. \quad (2.1.9)$$

$$\Re(A) = \left\{ (w_0^A - w_4^A) + \frac{1}{\sqrt{2}} [(w_1^A + w_7^A) - (w_3^A + w_5^A)] \right\} + \sqrt{-1} \left\{ (w_2^A - w_6^A) + \frac{1}{\sqrt{2}} [(w_1^A - w_7^A) + (w_3^A - w_5^A)] \right\} \\ \text{when } A \text{ is a sequence over } Z_8. \quad (2.1.10)$$

The crosscorrelation function between A and B is then becomes

$$C_{AB}(\tau) = \Re(\phi(A) - T^\tau \phi(B)), \quad (2.1.11)$$

where  $T^\tau(\cdot)$  is the  $\tau^{\text{th}}$  shift of  $(\cdot)$  and  $X - Y$  represents pointwise sequence subtraction modulo  $Z_M$ . Hence the computations of crosscorrelations reduce to calculation of weight vectors associated with the corresponding difference of  $Z_M$  sequences.

2. *Hamming correlation:* Here  $\phi$  is a mapping from a finite alphabet  $\mathcal{A}$  to another  $\mathcal{A}$  and the binary operation  $f$ , is given by

$$f(a, b) = 1 \text{ if } a = b \\ = 0 \text{ otherwise} \quad (2.1.12)$$

Then, as in the previous case, the Hamming correlation transform of a sequence A, is given by

$$\Re^H(A) = \sum_{i=0}^{N-1} f(a_i, 0) \quad (2.1.13)$$

Let  $W^A$  be the weight vector associated with A.  $\Re^H(A)$  is then

$$\Re^H(A) = W_0^A \quad (2.1.14)$$

The Hamming correlation between two sequences A and B is given by

$$HC_{AB}(\tau) = \Re^H(\phi(A) - T^\tau \phi(B)). \quad (2.1.15)$$

This correlation function is useful in environments where large sets of mutually orthogonal signals are employed in the modulation scheme. Some of the examples are frequency hopping systems, pulse position modulated systems etc.

3. *Block Inner-Product (BIP) correlation:* Here the elements of an alphabet  $\mathcal{A}$  over which sequences are defined is a collection of symbols from a smaller alphabet  $q$ . i.e.  $\mathcal{A} = q^r$

$$\text{if } A \in \mathcal{A}, A = (a_1 a_2, \dots, a_r); a_r \in q. \quad |\mathcal{A}| = |q|^r.$$

In this case  $\phi$  is a mapping from alphabet  $\mathcal{A}$  to  $r$ -tuples over complex number (signal space in this case



is a  $r$ -dimensional vector space over complex field) given by

$$\phi: \mathcal{A} \longrightarrow \mathbb{C}^r$$

$$\phi^B(A) = \phi^B(a_1, a_2, \dots, a_r) = \bar{\phi}(a_1), \bar{\phi}(a_2), \dots, \bar{\phi}(a_r), \quad (2.1.16)$$

where  $\bar{\phi}$  is the IP mapping (2.1.3),  $\bar{\phi}(a_1) = \exp\left(\frac{j2\pi\phi'(a)}{M}\right)$  and  $\phi'$  is a mapping from  $q$  to  $Z_M$ . The Binary operation  $f$  is given by

$$f^B(A, B) = A^T \cdot B^* = (a_1 b_1^* + a_2 b_2^* + \dots + a_r b_r^*), \quad (2.1.17)$$

where  $T$  represents transpose operation,  $b^*$  is the complex conjugate of  $b$  and  $\cdot$  is the symbol for dot product.

Binary and quaternary block inner-product correlations are particular cases of this correlation when range of the mapping  $\phi^B$  is  $r$ -tuples over  $2^{nd}$  and  $4^{th}$  roots of unity respectively. Also, inner-product correlation discussed previously is a particular case of BIP with block length  $r$  equal to 1.

The  $p$ -ary BIP correlation,  $p$  being a prime, is discussed specifically in this thesis where the sequence alphabet considered is residue class polynomial ring  $P_p^n[w(\xi)]$ ;  $w(\xi)$  is a polynomial of degree  $n$  over  $GF(p)$ . The mapping function  $\phi$  in this case becomes

$$\phi(a) = \phi(a_0, a_1, \dots, a_{n-1}) = \bar{\phi}(a_0), \bar{\phi}(a_1), \dots, \bar{\phi}(a_{n-1}), \quad (2.1.18)$$

where  $\bar{\phi}$  is the IP mapping,  $\bar{\phi}(x) = \exp\left(\frac{j2\pi x}{q}\right)$ , and  $a = (a_0, a_1, \dots, a_{n-1}) \in P_p^n[w(\xi)]$ . Thus a sequence over  $P_p^n[w(\xi)]$  is made up of  $n$  sequences over  $GF(p)$ . If  $A$  is a sequence over  $P_p^n[w(\xi)]$ , let  $A^j$  be the  $j^{th}$  component sequence over  $GF(p)$ , given by  $A^j = \{a_{j,i}, 0 \leq i \leq L-1\}$ ,  $0 \leq j \leq n-1$ . Then the correlation transform of  $A$  is given by

$$\begin{aligned} \kappa^{BIP}(A) &= \text{dot product of } \phi(A) \text{ and an all one vector.} \\ &= \sum_{i=0}^{L-1} \sum_{j=0}^{n-1} \bar{\phi}(a_{i,j}) = \sum_{j=0}^{n-1} \kappa^{IP}(A^j) \end{aligned} \quad (2.1.19)$$

Thus  $\kappa^{BIP}$  of a vector sequence is equal to sum of  $\kappa$ 's of its component sequences.

4. *Block Hamming correlation:* As in the previous case, sequence alphabet  $\mathcal{A}$  is a collection of symbols from smaller alphabet  $q$  and  $\phi$  is mapping from  $r$ -tuples over  $q$  to  $r$ -tuples over  $q'$ . The binary operation  $F(A, B)$ , is given by

$$F(A, B) = \sum_{i=0}^r f(a_i, b_i); A = (a_1, a_2, \dots, a_r), B = (b_1, b_2, \dots, b_r), \quad (2.1.20)$$

where  $f(a, b)$  is the binary operation defined for Hamming correlation.

5. *Lee Correlation*: Here  $\phi$  is a mapping from  $\mathcal{A}$  to signal alphabet  $Z_M$  and the binary operation  $f(a,b)$  is given by

$$f(a,b) = \lfloor M/2 \rfloor - \text{Lee}(a,b), \quad (2.1.21)$$

where  $\lfloor x \rfloor$  represents greatest integer less than or equal to  $x$ , and  $\text{Lee}(a,b)$  is the lee distance between  $a$  and  $b$  which is equal to minimum  $|a-b|$  or  $|b-a|$ ;  $|\cdot|$  is the modulus symbol.

Let  $A, B$  be two sequences over  $\mathcal{A}$ . Then the Lee correlation function is given by

$$\text{LC}_{AB}(\tau) = \sum_{i=0}^{N-1} \lfloor M/2 \rfloor - |\phi(a_i) - \phi(b_{i+\tau})|.$$

Let  $W_A$  be weight vector associated with vector  $\phi(A)$  such that  $W_i$  is number of symbols  $i$  in  $\phi(A)$ . Then  $\text{LC}_{AB}(\tau)$  is given by

$$\begin{aligned} \text{LC}_{AB}(\tau) &= \lfloor M/2 \rfloor W_0 + \sum_{i=1}^{\lfloor M/2 \rfloor} (\lfloor M/2 \rfloor - i) (W_i + W_{M-i}) \text{ when } M \text{ is odd} \\ \text{LC}_{AB}(\tau) &= \lfloor M/2 \rfloor W_0 + \sum_{i=1}^{\lfloor (M-1)/2 \rfloor} (\lfloor M/2 \rfloor - i) (W_i + W_{M-i}) \text{ when } M \text{ is even.} \end{aligned}$$

Correlation functions discussed above have close relationship with their corresponding distance measures used to define them. In fact correlation function is a measure of closeness of sequences. Let  $A, B$ , and  $C$  be three sequences of length  $L$  such that  $d(A,B) \geq d(A,C)$ , then correlation relation  $C_{AB}(0) \leq C_{AC}(0)$  always holds; where  $d(A,B)$  is the corresponding distance measure in a space of dimension  $L$  over which sequences are defined. Higher correlation value implies that the distance between sequences is small and conversely lower the correlation value they are far apart in corresponding metric space. Various correlation functions given above with their corresponding distance measures are given in Table 2.1.1.

## 2.2 More on Finite Rings Matched to Signal Set for Correlation

In Section 2.1, we have defined a generalized correlation function to take care of various correlation functions of practical importance. Correlation properties of sequences fall under secondary properties in the structural approach for construction of sequences. Analysis of sequences for secondary properties poses formidable problems. In an attempt to ease the secondary analysis, notion of sequence alphabet matched to a signal set for a correlation function represented by 2-tuple  $(f, \phi)$  has been proposed in Section 1.2. For convenience, we repeat the definition here.

**Definition 2.2.1:** A finite ring  $\mathcal{R}$  is said to be matched to a signal set for correlation represented by a 2-tuple  $(f, \phi)$  if and only if

$$f(\phi(a), \phi(b)) = f(\phi(a-b), \phi(0)), \text{ for any } a, b \in \mathcal{R}, \quad (2.2.1)$$

where  $-$  is the subtraction in finite ring  $\mathcal{R}$ .

The mapping  $\phi$ , which acts as a bridge between a finite ring and signal set, may be considered as an abstract modulator. A correlation function is defined on L tuples over a finite ring. Accordingly, the

**Table 2.1.1 Table of Correlation Functions & Corresponding Distance Measures**

Correlation type	Modulation.	Distance Measure	Mapping	$f(a, b)$ .
M-ary IP	M-PSK	Euclidean	$\phi: \mathcal{A} \rightarrow \mathbb{C}$ $\phi(a) = \exp\left(\frac{j2\pi\phi'(a)}{M}\right)$ $\phi': \mathcal{A} \rightarrow \mathbb{Z}_M$	$ab^*$
Binary IP	BPSK	Euclidean	$\phi: \mathcal{A} \rightarrow \mathbb{R}$ $\phi(a) = (-1)^{\phi'(a)}$ , $\phi': \mathcal{A} \rightarrow \mathbb{Z}_2$	$ab$
QPSK IP	QPSK	Euclidean	$\phi: \mathcal{A} \rightarrow \mathbb{C}$ $\phi(a) = (\omega)^{\phi'(a)}$ , $\phi': \mathcal{A} \rightarrow \mathbb{Z}_2$	$ab^*$
Hamming	FSK	Hamming	$\phi: \mathcal{A} \rightarrow \mathcal{A}$	$= 1, \text{ if } a = b$ $= 0, \text{ otherwise}$
Lee	MPSK	Lee	$\phi: \mathcal{A} \rightarrow \mathbb{Z}_M$	$\lfloor M/2 \rfloor - \text{Lee}(a, b)$ $\text{Lee}(a, b) = \min\{ a-b ,  b-a \}$
Block Inner Product	Block MPSK	Euclidean	$\phi^B: \mathbf{q}^r \rightarrow \mathbb{C}^r$ $\mathbf{A} = (a_1 \dots a_r)$ $\phi^B(\mathbf{A}) = \phi(a_1) \dots \phi(a_r)$ $\phi(a) = \exp\left(\frac{j2\pi\phi'(a)}{p}\right)$ , $\phi': \mathcal{A} \rightarrow \mathbb{Z}_p$	$\mathbf{a}^T \cdot \mathbf{b}^*$ $\mathbf{T}$ : transpose $\cdot$ : dot-product
Block Hamming	Block Hamming		$\phi: \mathbf{q}^r \rightarrow \mathbf{q}^r$ $\mathbf{A} = (a_1 \dots a_r)$	$F(\mathbf{A}, \mathbf{B}) = \sum_{i=0}^r f(a_i, b_i)$ where $f = 1, \text{ if } a = b$ $= 0, \text{ if } a \neq b$

structure of sequence alphabet is that of  $L$  tuples over a finite ring. Many practical situations demand sequences to be periodic and sequence alphabet can be assumed to be closed under cyclic shifts. Thus we are essentially interested in cyclic modules over finite rings. The implication of a finite ring being a matched ring in correlation computation is given in the following theorem using correlation transform.

**Theorem 2.2.1:** If  $A$  and  $B$  are two sequences over a matched finite ring  $\mathcal{R}$  for correlation represented by 2-tuple  $(f, \phi)$ , then  $\tau^{\text{th}}$  crosscorrelation between them is given by the correlation transform of  $(A - T^\tau(B))$ , where  $-$  is the subtraction in  $\mathcal{R}$  and  $T^\tau(\cdot)$  represents  $\tau^{\text{th}}$  shift of  $(\cdot)$ .

**Proof:** From (2.1.1), (2.2.1),  $C_{AB}(\tau)$  can be written as

$$C_{AB}(\tau) = \sum_{i=0}^{L-1} f\{\phi(a_i), \phi(b_{i+\tau})\} = \sum_{i=0}^{L-1} f\{\phi(a_i - b_{i+\tau}), \phi(0)\},$$

which is nothing but the correlation transform of  $(A - T^\tau B)$  from (2.1.2) as required.  $\square$

The above theorem reduces the burden of crosscorrelation computation between a pair of sequences by way of evaluating only the correlation transform of their difference sequence. It may be noted that  $\mathcal{R}$  is a property of a sequence where as crosscorrelation function involves a pair of sequences. Thus, computation of correlation properties of sequences over matched rings is simplified by using combinatorial results concerning the correlation transform of sequences. Further, if the sequence set is linear, the correlation distribution turns out to be directly related to correlation transform distribution of sequences in the set, which can be easily evaluated in many situations. This simplification is possible due to the fact that the correlation operation on the signal set is isomorphic to subtraction in the matched ring and more importantly the isomorphic mapping is linear. This isomorphism is shown in Fig 2.2.1. This allows us to make use of linearity of sequences over matched ring alphabet for the computation of correlation properties. As a result, the generalization of the alphabet structure from finite field to finite ring, in many situations, permits us to retain the advantages of linearity, thus leading to simplicity in the analysis of sequences. Thus while constructing sequences using the structural approach, it is advantageous to consider matched structures. Further, sequences over matched rings may also have good properties. Many optimal families of sequences over matched residue class finite rings derived in this thesis confirm this belief. Now we verify some of the residue class rings considered in this thesis for their matched ring property to various correlation functions. For the ring  $Z_M$ , we have the following lemma.

**Lemma 2.2.1:** The ring  $Z_M$  is a matched finite ring for IP correlation and the existence of optimal  $M$ -phase sequences necessarily imply the existence of  $Z_M$  sequences with optimal IP correlations.

*Anything more definitive than A possible?*

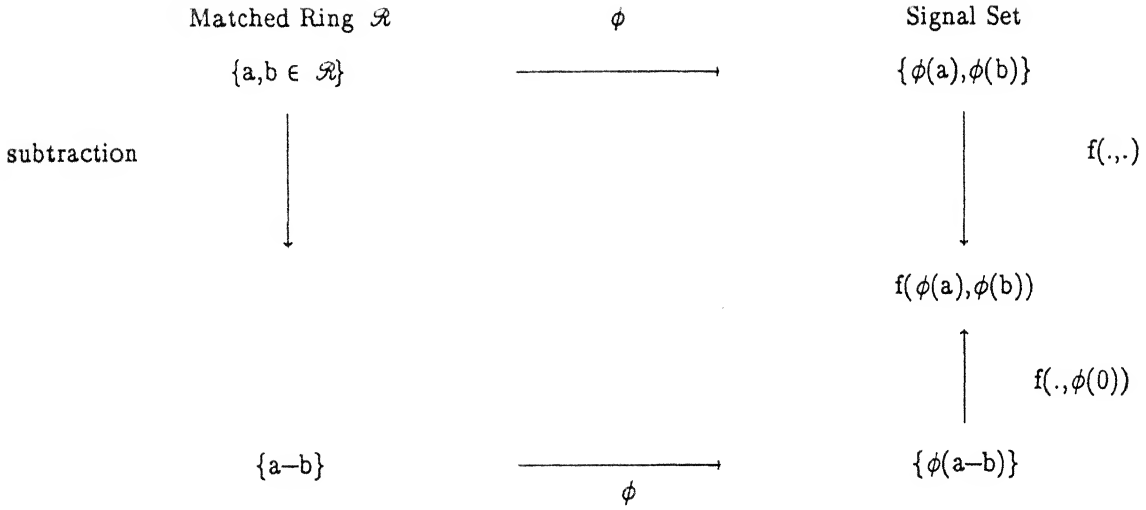


Fig 2.2.1 Relation between Matched Rings and Signal Sets

**Proof:** It is easy to see that  $Z_M$  satisfies (2.2.1), and hence a matched ring for IP correlations. Now note that the IP correlation involves a mapping  $\phi'$  from any arbitrary ring  $Q$  to  $Z_M$ . Thus if there exists a family of sequences  $F$  with optimal IP correlations over arbitrary ring  $Q$ , corresponding family of sequences  $\phi'(F)$  is a family of sequences over  $Z_M$  and is consequently optimal. Hence the lemma.  $\square$

Lemma 2.2.1 implies that  $Z_2$ ,  $Z_4$  and  $Z_8$  are matched rings for biphasic, quadriphase and octaphase IP correlations respectively. Lemma 2.2.1 implies only the existence of optimal sequences and do not suggest about the structure of optimal sequences. The fact that maximal length sequences over  $Z_4$  are optimal does not follow from the lemma. Another residue class ring considered in this thesis is residue class polynomial ring  $P_p^n[w(\xi)]$ . This ring is matched for block inner-product correlations and block Hamming correlations which can be verified easily. Table 2.2.1 gives some of the matched finite ring structures for various correlation functions.

## 2.3 Equivalence of Correlation Functions

In this section a concept of equivalence of correlation functions is discussed. The concept is motivated from implementing some correlation functions through the computation of equivalent correlation function.

**Definition 2.3.1:** Two correlation functions are said to be equivalent if the computation of correlation values from one correlation function is sufficient to determine the correlation values from the other function.

Theorem 2.3.1 shows that binary inner-product correlation and binary Hamming correlation are equivalent correlation functions. However such a correspondence does not hold good in general. Binary Hamming correlation is more easier to implement in digital domain [36] and thus the concept helps in implementing synchronization schemes for biphase sequences.

**Theorem 2.3.1:** Binary Hamming correlation is equivalent to binary inner-product type correlations.

**Proof:** Let A,B be two binary sequences of period L, then crosscorrelations between them according to both the correlation functions are given by

$$C_{AB}(\tau) \text{ (Inner-Product)} = \Re(A - T^T(B)) = w_0(\tau) - w_1(\tau) \quad (2.3.1)$$

$$HA_{AB}(\tau) \text{ (Hamming)} = \Re^A(A - T^T(B)) = w_0(\tau), \quad (2.3.2)$$

where  $w_0(\tau)$  and  $w_1(\tau)$  are the number of zeroes and ones respectively in the vector  $A - T^T(B)$ ,  $T^T(B)$ :  $\tau^{\text{th}}$  shift of B, and  $-$  indicates point wise subtraction. By using the fact that  $w_0(\tau) + w_1(\tau) = L$ , above correlation functions are rewritten as

$$C_{AB}(\tau) \text{ (Inner-Product)} = 2 HA_{AB}(\tau) - L \quad (2.3.3)$$

$$HA_{AB}(\tau) \text{ (Hamming)} = \frac{1}{2} (L + C_{AB}(\tau)) \quad (2.3.4)$$

Thus  $C_{AB}(\tau)$  and  $HA_{AB}(\tau)$  are proportional to each other and hence the result.  $\square$

**Table 2.2.1 Ring Structures Matched to Correlation Functions**

Sl No.	Matched Ring	Correlation Type
1.	$Z_M$	M-ary IP
2.	$Z_2 \equiv GF(2)$	Binary IP
3.	$Z_4$	Quadriphase IP
4.	Any Ring	Hamming
5.	$Z_M$	Lee
6.	$P_p^n[w]$	Block Inner-Product
7.	$P_p^n[w]$	Block Hamming

Above equivalence is not surprising because of the fact that the binary field is matched for both bi-phase IP correlation and Hamming correlation. Here Hamming distance between the elements of GF(2) is related to the euclidean distance between corresponding biphasic signals. This kind of equivalence is not true in general. Even though Lee distance between the elements of  $Z_M$  is related to euclidean distance between corresponding  $M^{\text{th}}$  roots of unity, Lee correlation is not equivalent to inner-product correlation, except in a special case  $M = 2$  where Lee correlation definition collapses to that of Hamming. By extending similar arguments it is easy to prove the following

**Theorem 2.3.2:** Binary block Hamming correlation is equivalent to binary block inner-product type correlations.

## 2.4 A Generalized Hamming Correlation Function

In Section 2.1, some of the commonly used correlation functions are obtained from a generalized correlation functions defined on sequences over arbitrary finite alphabet. In all these cases, distinguishability measure depends only on two sequences. Some communication practices demand correlation functions which depend on all sequences employed in the system. We consider such correlation functions called generalized Hamming correlation functions which are of importance in slow frequency hopping spread spectrum systems. They are defined as follows.

*Generalized Hamming correlation:* Let  $S^i$ ,  $m = 1, \dots, n$ , be  $n$  sequences of length  $L$  over certain alphabet  $Q$ , then the generalized Hamming crosscorrelation function concerning  $m^{\text{th}}$  sequence is given by

$$\text{GCH}_m(\tau_1, \tau_2, \dots, \tau_{m-1}, \tau_{m+1}, \dots, \tau_n) = \sum_{i=0}^{L-1} \text{gh}\{S^m_i; S^j_{i+\tau_j}, \text{ for all } j \neq m\}. \quad (2.4.1)$$

The corresponding autocorrelation function is given by

$$\text{GAH}_m(\tau_1, \tau_2, \dots, \tau_n) = \sum_{i=0}^{L-1} \text{gh}\{S^m_i; S^j_{i+\tau_j}, \text{ for all } j\} \quad (2.4.2)$$

where  $\text{gh}$  is a function given by

$$\begin{aligned} \text{gh}\{a; b_1, b_2, \dots, b_n\} &= 1 \text{ if } a \in \{b_1, b_2, \dots, b_n\} \\ &= 0 \text{ otherwise.} \end{aligned}$$

The use of above correlation function is discussed in Chapter 7. Families of sequences with ideal generalized correlation functions are given.

## 2.5 Criteria for Signal Design in Communication Systems

Requirements on the properties of sequences differ from one to application to another depending on the type of modulation, the channel, the presence of unintended intruders etc. A general and basic requirement is that sequences should have low out of phase autocorrelations and crosscorrelations. Various lower and upper bounds are present in the literature [1,34,35,41,70,71] which limits the performance of the systems. These are discussed in this section for various correlation functions. Apart from the limits on correlation values sequences should possess large linear complexity when threat of intentional jamming by unintentional user is present [5,61].

In case of single user systems where only one sequences has been made use of, autocorrelation functions are of prime importance. For multi-user systems both auto and crosscorrelations are important.

### 2.5.1 Inner-product Correlations

In case of inner-product type correlations, one of the important parameter which affects the performance is  $\theta_{\max}$  which is defined for a family of sequences  $F$  as maximum of out of phase autocorrelation values and crosscorrelation between different sequences in the family. Formally  $\theta_{\max}$  is given by

$$\theta_{\max} : \{\text{Max} (C_{XX}(\tau), \tau \neq 0, C_{XY}(\tau) \mid X \neq Y, X, Y \in F)\} \quad (2.5.1)$$

In addition to  $\theta_{\max}$ ,  $\theta_{\text{rms}}$  and  $\theta_{\text{avg}}$ , root mean square and average of all out of phase autocorrelations and crosscorrelations between all pair of sequences is also important in some occasions.

$\theta_{\text{rms}}$ : mean Square root of  $(|C_{XY}(\tau)|^2, \text{ for all } X, Y \in F, \text{ except when } X = Y \text{ \& } \tau = 0)$

$\theta_{\text{avg}}$ : average of  $|C_{XY}(\tau)|$ , for all  $X, Y \in F$ , except when  $X = Y \text{ \& } \tau = 0$ .

Formally these parameters are given by

$$\theta_{\text{rms}} = \frac{1}{M(ML-1)} \left( \sum_{\substack{X \in F \\ \text{except } X=Y \text{ \& } \tau \neq 0}} \sum_{Y \in F} \sum_{\tau=0}^{L-1} |C_{XY}(\tau)|^2 \right) \quad (2.5.2)$$

$$\theta_{\text{avg}} = \frac{1}{M(ML-1)} \left( \sum_{\substack{X \in F \\ \text{except } X=Y \text{ \& } \tau \neq 0}} \sum_{Y \in F} \sum_{\tau=0}^{L-1} |C_{XY}(\tau)| \right) \quad (2.5.3)$$

where  $M$  is the number of sequences in  $F$ .

For the above parameters bounds have been derived in the literature. Among them Welch bound on  $\theta_{\max}$  and  $\theta_{\text{rms}}$  and Sidelnikov bound on  $\theta_{\max}$  for biphasic sequences are popular. According to the Welch bound, for a collection of  $L$  complex valued sequences of period  $L$ ,  $\theta_{\max}$  cannot be less than a quantity that



is approximately  $\sqrt{L}$  [34]. However for biphasic sequences this cannot be better than  $\sqrt{2L}$  [35] (Sidelnikov bound).

In most of the sequence set constructions for CDMA operations, criteria often considered in literature is that,  $C_{\max}$  of the sequence set should be as small as possible. But in CDMA operations, it is not always necessary for the signal set to have minimum  $C_{\max}$ . Appropriate criteria is that the root mean square sum of the interference should be minimum ( $\theta_{\text{rms}}$  should be small) [41]. So in CDMA communication systems, one can afford to relax the requirement on  $C_{\max}$ , but it is required that the root mean square of the interference should be minimum. In fact, the Welch bound simply bounds the sum of square of crosscorrelations of all sequences in the set. Massey [41] has recently rederived the bound and gave the condition for a sequence set to satisfy welch bound with equality. Let  $X = \{x_m, m = 1, \dots, M\}$  be a set of  $M$  complex vectors of length  $L$  ( $x_m \in C^L$ ,  $L^{\text{th}}$  dimension complex space). Then the inner-product between the vectors  $x_m$  and  $x_n$  is given by

$$C_{mn}(0) = \sum_{i=1}^L (x_{mi} x_{ni}^*). \quad (2.5.4)$$

The energy of the vector  $x_m$  is defined as

$$E = \sum_{i=1}^L (x_{mi} x_{mi}^*). \quad (2.5.5)$$

Welch's bound theorem [41] bounds the inner-product values of the set  $X$ .

**Theorem 2.5.1: Welch's Bound:** If  $x_1, x_2, \dots, x_M$  are vectors of energy  $E$  in  $C^L$ , then a sum of inner-products satisfy

$$\sum_{n=1}^M \sum_{m=1}^M |C_{mn}(0)|^2 \geq \frac{(M E)^2}{L}, \quad (2.5.6)$$

where  $|x|$  means modulus value of  $x$ . Equality holds in the above equation, if and only if, in an  $M$  by  $L$  array having  $x_1, x_2, \dots, x_M$  as rows, the columns are mutually orthogonal and all columns have same energy.

Proof of the above theorem is given in Appendix E. The following theorem gives a method of constructing larger set of complex vectors satisfying Welch bound with equality from shorter sets which satisfy Welch bound with equality.

**Theorem 2.5.2:** If  $X = \{X_1, \dots, X_M\}$  and  $Y = \{Y_1, \dots, Y_N\}$  are two sets of complex vectors of length  $L$  satisfying Welch bound with equality, then the set  $Z = \{X \cup Y\}$  containing  $M+N$  complex vectors also satisfies the welch bound with equality, where  $\cup$  represents set theoretic union.

Proof: Let  $M_X$  and  $M_Y$  be matrices of  $M \times L$  and  $N \times L$  arrays whose rows are vectors in  $X$  and  $Y$  respectively. The sets  $X$  and  $Y$  satisfy Welch bound with equality implies

$$C_X^{ij} = 0 \text{ and } C_Y^{ij} = 0, \text{ for } i \neq j,$$

where  $C_X^{ij}$ ,  $C_Y^{ij}$  are the inner-products of  $i^{\text{th}}$  and  $j^{\text{th}}$  columns in  $M_X$  and  $M_Y$  respectively. Now consider,  $M_Z$  a  $M+N \times L$  matrix whose first  $M$  rows are vectors of  $X$  and next  $N$  rows are vectors of  $Y$ . Then inner-product between  $i^{\text{th}}$  and  $j^{\text{th}}$  columns,  $i \neq j$ , becomes

$$C_{XY}^{ij} = \sum_{m=1}^{M+N} (Z_{mi} Z_{mj}^*) = \sum_{m=1}^M (X_{mi} X_{mj}^*) + \sum_{m=1}^N (Y_{mi} Y_{mj}^*) = 0.$$

Hence the columns of  $M_Z$  are mutually orthogonal and thus  $Z$  satisfies Welch bound with equality.  $\square$

**Lemma 2.5.1:** If  $X$ , a set of  $M$  complex vectors of length  $L$  satisfying Welch bound with equality, then the set  $T^\tau(X)$ ,  $0 \leq \tau \leq L-1$ , also satisfy Welch bound with equality, where  $T^\tau(X)$  contains  $\tau^{\text{th}}$  shift of vectors in  $X$ .

Proof: Since  $T^\tau(X)$  contains  $\tau^{\text{th}}$  shift of vectors of  $X$ , column vectors of  $M_{T^\tau(X)}$  are  $\tau^{\text{th}}$  shift of those of  $M_X$  which are orthogonal. Thus, column vectors of  $M_{T^\tau(X)}$  are also mutually orthogonal which implies that  $T^\tau(X)$  also satisfies Welch bound with equality.

We say that a family of sequences  $F$  satisfies Welch bound with equality if set of vectors obtained by all shifts of sequences in  $F$  satisfies Welch bound with equality. Theorem 2.5.3 gives a consequence of a family of sequences satisfying Welch bound with equality.

**Theorem 2.5.3:** If  $F$ , a family of  $M$  sequences of period  $L$ , satisfies Welch bound with equality, then  $\theta_{\text{rms}}$  parameter for the family is given by

$$\theta_{\text{rms}} = \text{Square root } (M^2 E^2 - ML^2) / M(ML-1), \quad (2.5.7)$$

which is approximately equal to  $\sqrt{L}$  for sequences over roots of unity when  $M$  is of the order of  $L$ .

Proof: If  $F$  satisfies Welch bound with equality, then sets  $T^\tau(F)$ ,  $0 \leq \tau \leq L-1$  also satisfy Welch bound with equality. Then from Theorem 2.52,  $\{\bigcup_{\tau=0}^{L-1} T^\tau(F)\}$  also satisfies Welch bound with equality. This implies that

$$\sum_{n=1}^{ML} \sum_{m=1}^{ML} |C_{mn}(0)|^2 = \frac{(MLE)^2}{L}$$

where  $n$  and  $m$  runs through all the sequences in  $\{\bigcup_{\tau=0}^{L-1} T^\tau(F)\}$ . When  $m=n$ ,  $C_{mn}(0)$  is  $L$  and hence we have

$$\sum_{\substack{n=1 \\ n \neq m}}^{ML} \sum_{m=1}^{ML} |C_{mn}(0)|^2 = \frac{(MLE)^2}{L} - MLL^2 = M^2LE^2 - ML^3.$$

Since the vectors in  $\{\sum_{\tau=0}^{L-1} T^\tau(F)\}$  are all cyclic shifted versions of sequences in  $F$ , we have

$$\sum_{\substack{n=1 \\ n \neq m}}^{ML} \sum_{m=1}^{ML} |C_{mn}(0)|^2 = L \left( \sum_{\substack{X \in F \\ \text{except } X=Y \text{ \& } \tau \neq 0}} \sum_{Y \in F} \sum_{\tau=0}^{L-1} |C_{XY}(\tau)|^2 \right).$$

From (2.5.2) bracketed term in RHS of above equation is  $(1/ML(M-1))\theta_{rms}^2$ . Thus,  $\theta_{rms}^2$  becomes  $(M^2E^2 - ML^2)/ML(M-1)$  as required. This value is approximately equal to  $L$  if  $M$  is of the order  $L$ , and  $E = L$  which is the case when sequences are over roots of unity. Hence the theorem.  $\square$

Thus if a family satisfies Welch bound with equality, then it has optimal  $\theta_{rms}$ . Various families are derived in this thesis which have optimal  $\theta_{rms}$ .

## 2.5.2 Hamming Correlation

Hamming correlation function is useful in situations where large sets of mutually orthogonal signals are employed in modulation. Some of the examples are frequency hopping spread spectrum systems, multiple access communication systems based on FSK modulation and pulse position modulation systems. In such situations important parameters which affect the system performance are  $HA_{max}$  and  $HC_{max}$  which are defined as follows. Let  $\underline{F}$  be a family of sequences,  $HA_{max}$  and  $HC_{max}$  are given by

$$HA_{max} = \max_{A \in F} \{H_{AA}(\tau), \tau \neq 0\} \quad (2.5.8)$$

$$HC_{max} = \max_{A, B \in F} \{H_{AB}(\tau), \text{either } A \neq B \text{ or } \tau \neq 0\} \quad (2.5.9)$$

A good sequence design is the one which minimizes  $HC_{max}$ . Lempel and Greenberger [2] have derived lower bounds on the  $HA_{max}$  and  $HC_{max}$  for sequences over alphabet of size  $Q$  of period  $L$ . Families of sequences meeting this bound are called as optimal families of sequences.

Lower bounds on  $HA_{max}$  and  $HC_{max}$ : [2]

**Theorem: 2.5.4:** (Lempel and Greenberger [2]) Let  $A$  and  $B$  be two sequences of period  $L$  over an alphabet of size  $Q$ , and let  $W^A$  and  $W^B$  be weight vectors associated with  $A$  and  $B$  respectively. Then for a family of sequences  $\{A, B\}$

$$HA_{max} \geq (L-b)(L+b-Q)/Q(L-1) \quad (2.5.10)$$

where  $b$  is the least nonnegative residue of  $L \bmod Q$ , and

$$HC_{max} \geq (\beta - 2L)/(3L - 2) \quad (2.5.11)$$

where  $\beta = \sum_{i=0}^{Q-1} (w_i^A w_i^A + (w_i^A)^2 + (w_i^A)^2)$ . Note that we may assume  $w_1^A \geq w_2^A \geq w_3^A \geq \dots \geq w_Q^A$ , where  $w_i^A$  is the number of  $i^{\text{th}}$  symbol  $\alpha_i \in Q$ . Furthermore, the right hand side of (2.5.11) is minimized whenever the following conditions are satisfied

- 1)  $w_1^A - w_Q^A \leq 1$
- 2) the  $w_i^A$ 's are increasing order  $w_1^B \leq w_2^B \leq w_3^B \leq \dots \leq w_Q^B$ .
- 3)  $w_Q^B - w_1^B \leq 1$ .

For  $L = V^r - 1$  and  $Q = V^\rho$ , the above inequalities become [2]

$$HA_{\max} \geq V^{r-\rho} - 1 \quad (2.5.12)$$

$$HC_{\max} \geq V^{r-\rho}. \quad (2.5.13)$$

### 2.5.3 Linear Complexity

**Definition: Linear Complexity:** The linear complexity of a sequence  $S = \{s_i, i \in \mathbb{Z}_L\}$  of period  $L$  over any ring  $\mathcal{R}$  is defined as the least number stages required generate the sequence using linear feedback shift register (LFSR). A LFSR of length  $m$  is shown in Fig 2.5.1.

A LFSR of length  $m$  with initial loading  $s_0, s_1, \dots, s_{m-1}$  generates  $S$  if it follows linear recursion

$$s_{m+j} = - \sum_{i=1}^m c_{m-i} s_{m+j-i} \quad (2.5.14)$$

where  $c_0, c_1, \dots, c_{m-1}$  are the tap coefficients of the LFSR. The associated connection polynomial is  $C(x)$  given by  $c_0 + c_1 x + \dots + c_{m-1} x^{m-1} + x^m$ . Let  $S(x) = s_{L-1} + s_{L-2} x + s_{L-2} x^{L-2} + \dots + s_0 x^{L-1}$  be a polynomial associated with the sequence  $S$ . Then it is easy to verify that a LFSR with connection

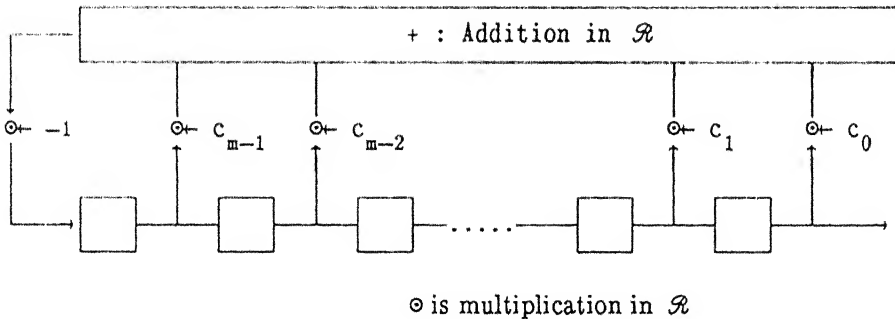


Fig 2.5.1 LFSR of Length  $m$

## Chapter 3

### Maximal Length and Allied Sequences over $Z_4$ and $Z_8$

This chapter is concerned with construction of maximal length and allied sequences over  $Z_{2^k}$  and their periodic correlation properties. Galois extension rings of  $Z_{2^k}$  play an important role in various constructions. Relevant algebraic properties of the Galois extension ring of  $Z_{2^k}$  are given in Appendix A. Families of sequences derived from maximal length sequences over  $Z_4$  which can be used in quadriphase modulated communication systems are discussed in detail. Families derived from sequences over  $Z_8$  can be used in octaphase modulated communication systems.

The chapter is organized as follows. Essential mathematical background required for the chapter is given in Section 3.1 and 3.2. Properties of Galois extension ring of  $Z_4$  of degree  $r$ , denoted as  $GR(4,r)$ , needed for the chapter, are briefly reviewed in Section 3.1. Relevant properties of an algebraic Abelian association scheme defined on the elements of  $GR(4,r)$  are given in Section 3.2. Families of trace function sequences are defined in Section 3.3. Trace functions (given in Appendix A) over  $GR(4,r)$  and the Abelian association scheme are used extensively in Sections 3.4 and 3.5 to define various families of quadriphase sequences and to obtain their correlation properties. Section 3.4 presents a family of  $L+2$  maximal length sequences ( $m$ -sequences) over  $Z_4$  of period  $L = 2^r - 1$ . The Abelian association scheme on the elements of  $GR(4,r)$  has been used to calculate crosscorrelation and out-of-phase autocorrelation values of sequences. Section 3.5 deals with the construction of sequences with period  $2(2^r - 1)$ . The correlations are computed from the analytical correlation expressions for  $m$ -sequences. Maximal length sequences over  $Z_8$  which can be used in octaphase communication systems are discussed in Section 3.6. Subsets of maximal length sequences over  $Z_8$  are identified which satisfy Welch bound with equality.

#### 3.1 Salient Features of Galois Ring $GR(4,r)$

This section briefly reviews essential structural properties of Galois ring of  $Z_4$  of degree  $r$ , denoted as  $GR(4,r)$ , as required for this chapter. Essential properties of general Galois ring  $GR(2^k,r)$  are given Appendix A.

P1: For every positive integer  $d$ , there is a natural inclusion of  $GR(4,r)$  into  $GR(4,dr)$ , similar to Galois fields [87,88]. In other words, every subring of  $GR(4,r)$  is of the form  $GR(4,s)$  for some divisor  $s$  of  $r$ . Conversely, for every positive divisor  $s$  of  $r$ , there is a unique subring  $R$  which is isomorphic to  $GR(4,s)$ .

P2: There is a natural homomorphic mapping, denoted by  $\hat{\cdot}$ , from  $GR(4,r)$  to  $GR(2,r)$  which takes  $GR(4,r)$  to the residue field  $GF(2^r)$ . It is given by  $\hat{a} = a \bmod 2$ ,  $a \in GR(4,r)$  [87,88].

P3: The only non-trivial ideal of  $GR(4,r)$  is the set of zero divisors in  $GR(4,r)$ , i.e.,  $\{0, 2, 2\alpha, 2\alpha^2, \dots, 2\alpha^{2^r-1}\}$ , where  $\alpha$  is an unit element of multiplicative order  $2^r-1$  in  $GR(4,r)$ . It is denoted by  $\langle 2 \rangle$  and is isomorphic to the finite field  $GF(2^r)$ . ✓

Proof: That  $\langle 2 \rangle$  is an ideal of  $GR(4,r)$  is easily verified. The result then follows from the fact that  $GR(4,r)$  is a local ring. □

P4: In  $GR(4,r)$ ,  $2\alpha = 0$  if and only if  $\alpha \in \langle 2 \rangle$ .

Proof: From the facts that  $\langle 2 \rangle$  is an ideal of  $GR(4,r)$  and that  $GR(4,r)$  is of characteristic 4. □

P5:  $GR(4,r) \setminus \langle 2 \rangle$ , where  $\setminus$  represents set theoretic subtraction, is the group of units of  $GR(4,r)$ , denoted by  $GR^*(4,r)$ .

Proof: Follows from P3 above. □

P6:  $GR^*(4,r)$  can be written as the direct product of two groups  $G_c$  and  $G_a$ ;  $GR^*(4,r) \cong G_c \otimes G_a$ , where  $G_c$  is a cyclic group of order  $2^r-1$  and  $G_a$  is an Abelian group of order  $2^r$ .  $G_a$  itself is a direct product of  $r$  cyclic groups, each of order 2; its elements are given by

$$\{1, (1+2(\alpha^i)); i = 0, 1, \dots, 2^r-1\} \quad (3.1.1)$$

where  $\alpha$  is a primitive element  $\in G_c$  whose multiplicative order is  $2^r-1$ . Since  $2\alpha^i \in \langle 2 \rangle$ , elements of  $G_a$  are alternatively given by the set

$$\{(1 + (\beta)); \beta \in \langle 2 \rangle \cong GF(2^r)\} \quad (3.1.2)$$

Also, for any  $a \in G_a$ ,  $a^2 = 1$  (identity of the ring) and thus there are exactly  $2^r$  cyclic subgroups order 2.

P7: Every unit element  $u$  belonging to  $GR^*(4,r)$  may be written as  $a\alpha$ , where  $a \in G_a$ ,  $\alpha \in G_c$ .

**Proof:** Follows from structure of  $GR^*(4,r)$ .  $\square$

P8: Every non-zero element of  $GR(4,r)$  may be written as  $u*2^t$ , where  $u$  is a unit and  $t$  is either 0 or 1.

In this representation  $t$  is unique and  $u$  is unique modulo  $(2^{2-t})$ .

**Proof:** Follows from structure of  $GR^*(4,r)$ , and P3, P4, and P5 given above.  $\square$

P9:  $G_c$  is the set of non-zero squares in  $GR(4,r)$ .

**Proof:** Follows from the structure of  $GR^*(4,r)$ , and the fact that square of any element of  $G_a$  is unity.  $\square$

P10: By using the natural ring homomorphism from  $GR(4,r)$  to  $GF(2^r)$  ( $\bar{\cdot}$  : reduction modulo 2), the elements of  $G_a$  are given by the set

$$\{1, (1 + 2(\hat{\alpha}))\alpha \in G_c\} = \{(1 + 2(\beta))\beta \in GF(2^r)\} \quad (3.1.3)$$

If  $a_i \in G_a$ ;  $i = 1, 2, \dots, r$ , then  $\prod_{i=1}^r a_i = 1 + \sum (a_i - 1) = 1 + 2(\sum \hat{a}_i)$ , where  $\hat{a}_i = (1 + 2a_i')$ . Hence, the multiplication in  $G_a$  is related to the addition in  $GF(2^r)$ . Also the representation of (3.1.3) induces an isomorphism between  $G_a$  and the residue field  $GF(2^r)$ . This isomorphic mapping from  $G_a$  to  $GF(2^r)$  is denoted by  $\bar{\cdot}$ , ie. if  $a = (1 + 2a')$ , then  $\bar{a} = \hat{a}' \in GF(2^r)$ .

P11: Product representation of  $G_a$ : Let  $\{1, \beta_1\}, \{1, \beta_2\}, \dots, \{1, \beta_r\}$  be  $r$  cyclic component subgroups of  $G_a$  such that  $G_a = \{1, \beta_1\} \otimes \{1, \beta_2\} \otimes \dots \otimes \{1, \beta_r\}$ , where  $\otimes$  denotes direct product symbol. Then for any  $a \in G_a$  has a product representation  $(a_0, a_1, \dots, a_{r-1})$  with  $\beta_1, \beta_2, \dots, \beta_r$  as basis, such that

$$a = (\beta_1)^{a_0} (\beta_2)^{a_1} \dots (\beta_r)^{a_{r-1}}, \text{ where } a_i \text{ are either 0 or 1.} \quad (3.1.4)$$

**Proof:** Follows from the direct product structure of  $G_a$ .  $\square$

P12: Condition for a set of elements of  $G_a$  to constitute a basis for product representation: The subgroups  $\{1, \beta_1\}, \{1, \beta_2\}, \dots, \{1, \beta_r\}$  are component subgroups of  $G_a$  of order 2, if and only if set of elements  $\{\tilde{\beta}_1, \tilde{\beta}_2, \dots, \tilde{\beta}_r\}$  constitutes a basis in  $GF(2^r)$ , where each  $\beta_i = (1 + 2\tilde{\beta}_i)$ .

**Proof:** Follows from the isomorphism  $\bar{\cdot}$  between  $G_a$  and residue field  $GF(2^r)$ . Note that the multiplication of any two elements from  $G_a$  is same as the addition of the corresponding elements of  $GF(2^r)$ .  $\square$

P13: Let the elements  $1, \alpha, \dots, \alpha^{r-1}$  be standard basis elements of  $GF(2^r)$ . Then from the P10, the sets  $\{1, 1+2\}, \{1, 1+2(\alpha)\}, \dots, \{1, 1+2(\alpha^{r-1})\}$  are cyclic component subgroups of  $G_a$  and hence any element of  $G_a$  can be written as

$$a = (3)^{a_0} (1+2(\alpha))^{a_1} \dots (1+2(\alpha^{r-1}))^{a_{r-1}} \quad (3.1.5)$$

where  $a_i$  are either 0 or 1. This representation is called standard product representation of  $G_a$  analogous to the standard basis representation of  $GF(2^r)$ .

P14: Finding a product representation of  $G_a$  given a basis element  $\beta_1 = \gamma$ : Here the problem is to choose remaining elements  $\beta_2, \dots, \beta_r$ , such that elements  $\tilde{\gamma}, \tilde{\beta}_2, \dots, \tilde{\beta}_r$  constitute a basis for  $GF(2^r)$ . These elements are derived from the standard basis representation of  $\tilde{\gamma}$  as follows. Let  $\tilde{\gamma}$ , in the standard basis representation, be equal to  $\tilde{\gamma} = \gamma_0 + \gamma_1 \alpha^1 + \dots + \gamma_{r-1} \alpha^{r-1}$ , where  $\gamma_i$  are either 0 or 1. By collecting  $\gamma_i$ 's which have a value 1,  $\tilde{\gamma}$  can be written as  $\tilde{\gamma} = \gamma_{i1} \alpha^{i1} + \gamma_{i2} \alpha^{i2} + \dots + \gamma_{it} \alpha^{it}$ , where  $\gamma_{ij} = 1; 1 \leq j \leq t$ , and  $\gamma_{ij} = 0; j > t$ . Now choose  $\tilde{\beta}_2 = \alpha^{i2}, \dots, \tilde{\beta}_t = \alpha^{it}, \tilde{\beta}_{t+1} = \alpha^{it+1}, \dots, \tilde{\beta}_r = \alpha^{ir}$ . It can be verified that the set  $\{\tilde{\gamma}, \tilde{\beta}_2, \dots, \tilde{\beta}_r\}$  constitutes a basis for  $GF(2^r)$ . Hence, any  $a \in G_a$ , can be expressed as

$$a = (\gamma)^{a_0} (\beta_2)^{a_1} \dots (\beta_r)^{a_{r-1}} \quad (3.1.6)$$

A trace function maps elements of  $GR(4, r)$  to one of its intermediate subrings. The definition and properties of trace functions are given in Appendix A. Following definition of trace number of any unit element will be useful later.

**Definition 3.1.1:** Trace number: The trace number associated with any unit element  $u = a\alpha$ ,  $a \in G_a$ ,  $\alpha \in G_c$ , is defined as value of  $\text{tr}_1^r(\tilde{a})$ , where  $\tilde{a}$  represents the isomorphism between  $G_a$  and  $GF(2^r)$ . It is either 0 or 1.

## 3.2 Association Schemes on Abelian Groups

Definition and relevant results of Abelian association schemes are given in this section. For more details on Abelian association schemes refer [22, 24, 89, 90,]. An association scheme defined on the elements of  $GR(4, r)$  is considered and its relevant properties are given. This scheme has been used extensively in Sections 3.4 and 3.5 for computing correlation properties of various families of sequences.



**Definition 3.2.1:** An Abelian association scheme with  $n+1$  classes on a Abelian group  $G$ , denoted by  $(G, \Gamma)$ , partitions cartesian square  $G^2$  (set of all 2-tuples over  $G$ ) into  $n+1$  classes  $\Gamma_0, \Gamma_1, \dots, \Gamma_n$  ( $\Gamma_0$  being the diagonal class given by  $\{(x, x); x \in G\}$ ) satisfying following conditions.

- i. Given  $x \in G$ , the number  $v_i$  given by  $|\{(x, y) \in \Gamma_i, y \in G\}|$  depends only on  $i$ , where  $|\{.\}|$  represents cardinality of the enclosed set  $\{.\}$
- ii. Given  $x, y \in G$  with  $(x, y) \in \Gamma_k$ , the number given by  $|\{(x, z) \in \Gamma_i \text{ and } (y, z) \in \Gamma_j, z \in G\}|$  is a constant  $p_{i,j}^k$  depending only on  $i, j$ , and  $k$ .
- iii. The classes are invariant under translation in  $G$  i.e.  $(x, y) \in \Gamma_i \Rightarrow (x+z, y+z) \in \Gamma_i$ .

If a 2-tuple  $(x, y) \in \Gamma_i$ , then  $x$  and  $y$  of  $G$  are called as  $i^{\text{th}}$  associates.

It is convenient to represent these classes by adjacency matrices. The adjacency matrix corresponding to the class  $\Gamma_i$  is of size  $|G|$  and is denoted by  $D_i$ . The entries  $D_i(x, y); x, y \in G$ , are equal to one if  $(x, y) \in \Gamma_i$  and are zero otherwise. Thus  $D_0$  is the identity matrix  $I$  of order  $|G|$ . In view of condition (ii), the  $(x, y)^{\text{th}}$  entry in the matrix product  $D_i D_j$  or  $D_j D_i$  is given by  $p_{i,j}^k$  if  $(x, y) \in \Gamma_k$ . Thus we can write

$$D_i D_j = D_j D_i = \sum_{k=0}^n p_{i,j}^k D_k \quad (3.2.1)$$

The commuting matrices  $D_0, D_1, \dots, D_n$  span  $n+1$  dimensional algebra, called Bose–Mesner (B–M) algebra [22,89,90].

### 3.2.1 Characters of Finite Abelian Groups

A character  $\chi$  of a finite Abelian group  $G$  is a homomorphism of  $G$  into the multiplicative group of complex roots of unity. i.e.  $\chi(x+y) = \chi(x)\chi(y)$  holds for all  $x, y \in G$ . The set  $G'$  of all characters, constitutes a group isomorphic to  $G$  with respect to multiplication defined as follows:

$$\text{for } \chi, \psi \in G', (\chi \psi)(x) = \chi(x) \psi(x), \text{ for all } x \in G.$$

The image of  $x \in G$  under the isomorphism  $G \longrightarrow G'$  is denoted by  $\chi_x$  so that  $\chi_x \chi_y = \chi_{x+y}$  for every  $x, y \in G$ . Thus

$$\begin{aligned} \chi_{x+y}(z) &= \chi_x(z) \chi_y(z), \\ \chi_x(y+z) &= \chi_x(y) \chi_x(z), \text{ for all } x, y, z \in G. \end{aligned} \quad (3.2.2)$$

Let  $S$  denote the square matrix of order  $|G|$  with entries  $\chi_x(y)$  indexed by the elements  $x, y \in G$ . From the orthogonality relations satisfied by the characters of  $G$ , it is easy to show that  $S \tilde{S} = \tilde{S} S = |G| I$ , where  $\tilde{S}$  is the conjugate transpose of  $S$ . Theorem 3.2.1 gives eigenvectors of Abelian association scheme on  $G$

**Theorem 3.2.1** [90]: All the matrices in the B-M algebra (of adjacency matrices  $\{D_k, k \in X\}$  of the Abelian association scheme on  $G$  have the same set of eigenvectors. They are given by the columns of  $S$ . The  $z^{\text{th}}$  eigenvalue of  $D_k$  is given by

$$P_k(z) = \sum_{u \in \Gamma_k} \chi_u(z); z \in G. \quad (3.2.3)$$

**Proof:** It is sufficient to prove the above result for the adjacency matrix  $D_k$  of the Abelian scheme. From Definition 3.2.1 (Part iii) and (3.2.2) we have,  $\sum_{y \in G} D_k(x,y) \chi_y(z) = \sum_{u \in \Gamma_k} \chi_{x+u}(z) = \chi_x(z) \sum_{u \in \Gamma_k} \chi_u(z)$ .

Hence the  $z^{\text{th}}$  column vector in  $S$  is an eigenvector of  $D_k$ . The corresponding eigenvalue is given by the summation  $\sum \chi_u(z)$  over all  $u \in \Gamma_k$ .  $\square$

### 3.2.2 An Association Scheme Defined on the Elements of $GR(4,r)$

We consider an association scheme with the elements of  $GR(4,r)$  as the points of the scheme. The classes of the scheme depend on the following partition of  $GR(4,r)$

1.  $2^r$  subsets corresponding to each elements of  $G_a$ :

$$[a] = a^*(G_c); a \in G_a, \quad (3.2.4a)$$

where  $G_c$  and  $G_a$  are cyclic and Abelian component subgroups of  $GR^*(4,r)$ , the group of units of  $GR(4,r)$ , of order  $2^r-1$  and  $2^r$  respectively.

2. A subset consisting of proper zero divisors:  $[e] = \langle 2 \rangle - \{0\}$  (3.2.4b)

3. The zero subset:  $[\omega] = \{0\}$ . (3.2.4c)

The  $2^r+2$  subsets in (3.2.4) partition  $GR(4,r)$  corresponding to the equivalence relation  $\alpha \cong \beta$  if and only if  $\alpha G_c \cong \beta G_c$ .  $2^r+2$  classes ( $X$ ) are defined corresponding to  $2^r+2$  subsets in (3.2.4); two elements  $\alpha, \beta \in GR(4,r)$  are called  $x^{\text{th}}$  class associates,  $(\alpha, \beta) \in \Gamma_x$ , if  $\alpha - \beta \in [x]$ . The scheme is denoted by  $(GR(4,r), X)$ . Note that in the scheme  $(GR(4,r), X)$ ,  $(\alpha, \beta) \in \Gamma_x \Rightarrow (\alpha + \delta, \beta + \delta) \in \Gamma_x$ ;  $\alpha, \beta, \delta \in GR(4,r)$ . Thus the scheme  $(GR(4,r), X)$  with  $2^r+2$  classes is accordingly an Abelian scheme on the elements of  $GR(4,r)$  (written additively) which is invariant under translation in  $X$ . Characters of the Abelian group  $GR(4,r)$  are given by

$$\chi_y(x) = \omega^{\text{tr}(xy)}; \omega = \sqrt{-1}, x, y \in GR(4,r) \quad (3.2.5)$$

Let  $I, E$  (corresponding to classes  $[\omega]$  and  $[e]$  respectively), and  $A_a$  for each  $a \in G_a$  be the adjacency matrices of size  $4^r$  of the Bose-Mesner (B-M) algebra of the scheme. Liebler and Mena [40] have

computed the relations connecting the adjacency matrices of the B-M algebra in the context of constructing certain distance regular graphs of girth 4.

For  $a, b, c \in X$ , define  $n(a,b;c)$  to be the number of times a fixed element of class  $[c]$  occurs in the Caley table of  $[a]+[b]$ . This number is independent of the element of  $[c]$  that is chosen, since in  $\langle [a]+[b] \rangle$ , the occurrence of any element of  $[c]$  implies the occurrence of all the elements of  $[c]$ . The commutative property of  $GR(4,r)$  implies  $n(a,b;c) = n(b,a;c)$ . Various structural constants  $n(a,b;c)$ ,  $a, b, c \in X$ , are computed in [40], and they are reproduced in the following Lemma 3.2.1 below without proof. The constants given in Lemma 3.2.1 are the intersection numbers of the scheme:  $n(a,b;c) = p_{ab}^c$ .

**Lemma 3.2.1:** (Liebler and Mena) [40]

- 1)  $n(w,w; x) = \begin{cases} 0 & \text{if } w \neq x \\ 1 & \text{if } w = x. \end{cases}$
- 2)  $n(e,e,x) = \begin{cases} 0 & \text{if } x \neq e, w \\ 2^r - 1 & \text{if } x = w \\ 2^r - 2 & \text{if } x = e \end{cases}$
- 3)  $n(e,a; x) = \begin{cases} 0 & \text{if } x = a, e, \text{ or } w \quad \text{for any } a \in G_a \\ 1 & \text{if otherwise} \quad \text{for any } a \in G_a^a \end{cases}$
- 4)  $n(a,b; w) = \begin{cases} 2^r - 1 & \text{if } b = 3a \quad \text{for any } a, b \in G_a \\ 1 & \text{otherwise} \quad \text{for any } a, b \in G_a^a \end{cases}$
- 5)  $n(a,b; e) = \begin{cases} 0 & \text{if } b = 3a \quad \text{for any } a, b \in G_a \\ 1 & \text{otherwise} \quad \text{for any } a, b \in G_a^a \end{cases}$
- 6)  $n(0,0;0) = 0$ .
- 7) if  $a,b,c,d \in G_a$ , then  $n(a,b;c) = n(ad,bd;cd)$ .
- 8) Let  $a,b \in G_a$ . Then  $n(a,3a; b) = \begin{cases} 0 & \text{if } b = a, 3a \\ 1 & \text{otherwise} \end{cases}$ .
- 9) Let  $a,b \in G_a$ ,  $a \neq b$ . Then  $n(a,a; b) = \begin{cases} 2 & \text{if } \text{tr}(\tilde{b}) = \text{tr}(\tilde{a}) \\ 0 & \text{otherwise} \end{cases}$ .
- 10) Let  $a,b,c \in G_a$ ,  $a \neq b, 3b$ . Then
 
$$n(a,b;c) = \begin{cases} 1 & \text{if } c = a, b. \\ 2 & \text{if } c \neq a, b, \text{tr}(\tilde{a}\tilde{b} + \tilde{a}\tilde{c} + \tilde{b}\tilde{c}) = \text{tr}(\tilde{c}). \\ 0 & \text{otherwise} . \end{cases}$$

where  $\tilde{\phantom{x}}$  represents the isomorphism between  $G_a$  and  $GF(2^r)$ .

Using (3.2.1) and intersection numbers given in Lemma 3.2.1, following matrix equations connecting adjacency matrices of the scheme  $(GR(4,r), X)$  are derived in [40].

**Lemma 3.2.2:** (Liebler and Mena) [40]: For each  $a \in G_a$

$$1) A_a^T = A_{3a}, E = E^T, EJ = JE = A_a J = JA_a = (2^r - 1)J \quad (3.2.6)$$

$$2) E^2 = (2^r - 1)I + (2^r - 2)E \quad (3.2.7)$$

$$3) A_a E = J - I - E - A_a \quad (3.2.8)$$

$$4) A_a A_a^T = (2^r - 2)I + J - E - A_a - A_a^T \quad (3.2.9)$$

$$5) A_a^2 = E + 2 \sum_{a \neq b} \text{tr}(\tilde{a}) = \text{tr}(\tilde{b}) A_b, \quad (3.2.10)$$

where  $\tilde{\phantom{x}}$  represents the isomorphism between  $G_a$  and  $GF(2^r)$  and  $J$  is the all 1 matrix of size  $4^r$  by  $4^r$ .

Additional results needed on adjacency matrices are given in Lemmas 3.2.3 and 3.2.4.

**Lemma 3.2.3:** For all  $a \in G_a$ ,

$$1) A_a A_{a\gamma} = E - (A_a + A_{a\gamma}) + 2 \left( \sum_{c \in G_a} A_c \right), \quad (3.2.11)$$

$\gamma \neq 1, 3$

where  $c$ 's are such that  $\text{tr}(\tilde{a}(\tilde{\gamma} + \tilde{a}) + \tilde{\gamma}\tilde{c}) = \text{tr}(\tilde{c})$ .

$$2) \sum_{a \in G} A_a = J - (I + E) \quad (3.2.12)$$

$$3) \sum_{a \in G_a} A_a A_{a\gamma} = 2^r E + (2^r - 2)(J - I - E); \gamma \neq 1, 3 \quad (3.2.13)$$

where  $\tilde{\phantom{x}}$  is the isomorphism between  $G_a$  and the residue field  $GF(2^r)$ .

**Proof:** (3.2.11) follows from Lemma 3.2.1 (Part 10) and (3.2.1). (3.2.12) is true, since,  $\sum A_a = J$ , the matrix of all 1's. Substituting  $a = 1$ , in (3.2.11) gives  $A_1 A_{1\gamma} = E - (A_1 + A_{1\gamma}) + 2 \left( \sum_{c \in G_a} A_c \right)$ , where  $c$ 's

are such that  $\text{tr}(\tilde{\gamma}\tilde{c}) = \text{tr}(\tilde{c})$ . Then by using Lemma 3.2.1 (Part 7),  $A_a A_{a\gamma}$  can be written as  $A_a A_{a\gamma} = E - (A_a + A_{a\gamma}) + 2 \left( \sum_{c \in G} A_{ca} \right)$ , where  $c$ 's are such that  $\text{tr}(\tilde{\gamma}\tilde{c}) = \text{tr}(\tilde{c})$ . Taking summation of  $A_a A_{a\gamma}$  over all the elements of  $G_a$ , and using (3.2.12) readily yield (3.2.13).  $\square$

Let  $G_a(0^{-1})$  be the set consisting of all those elements of  $G_a$  whose trace number is 0. This set is closed under multiplication. Similarly, let  $G_a(1^{-1})$  be the set consisting of all those elements of  $G_a$  whose trace number is 1.

**Lemma 3.2.4:** For  $\gamma \neq 1, 3$  with  $\text{tr}(\tilde{\gamma}) = 0$ ,

$$\sum_{a \in G_a(0^{-1})} A_a A_{a\gamma} = (2^{r-1})(J - I - E) + 2^{r-1} E - \sum_{a \in G_a(0^{-1})} 2A_a \quad (3.2.14)$$

$$\sum_{a \in G_a(1^{-1})} A_a A_{a\gamma} = (2^{r-1})(J - I - E) + 2^{r-1} E - \sum_{a \in G_a(1^{-1})} 2A_a \quad (3.2.15)$$

Proof: As in the proof of Lemma 3.2.3,  $A_a A_{a\gamma}$  can be written as

$$A_a A_{a\gamma} = E - (A_a + A_{a\gamma}) + 2 \left( \sum_{c \in G_a} A_{ca} \right), \quad (3.2.16)$$

where  $c$ 's are such that  $\text{tr}(\tilde{\gamma} \tilde{c}) = \text{tr}(\tilde{c})$ . The summation of the third term in the RHS of (3.2.16) over all  $a \in G_a(0^{-1})$  is given by  $\sum_{a \in G_a(0^{-1})} \left( \sum_{c \in G_a} A_{ca} \right)$ , where  $c$ 's such that  $\text{tr}(\tilde{\gamma} \tilde{c}) = \text{tr}(\tilde{c})$ . We first show that in the set of elements given by  $\{c, c \in G_a \text{ such that } \text{tr}(\tilde{\gamma} \tilde{c}) = \text{tr}(\tilde{c})\}$ , the number of elements with trace number 1 is equal to that with trace number 0. There are exactly  $2^{r-1}$  such elements because they are the solutions of the polynomial equation

$$(1 + \tilde{\gamma})x + (1 + \tilde{\gamma})^2 x^2 + \dots + (1 + \tilde{\gamma})^{2^{r-1}} x^{2^{r-1}} = 0 \quad (3.2.17)$$

over  $\text{GF}(2^r)$  of degree  $2^{r-1}$ . Also the solutions are closed under addition. Thus it is sufficient to show that there exists at least one  $\tilde{c}$  whose trace is one. Assume that trace of all solutions of (3.2.17) is equal to zero.

Then this implies that they are the solutions of a polynomial equation  $(x + x^2 + \dots + x^{2^{r-1}}) = 0$  over  $\text{GF}(2^r)$ . But they are also obtained as solutions of (3.2.17). This implies that  $\tilde{\gamma}$  is identically equal to 0, which contradicts the fact that  $\gamma \neq 1, 3$  ( $\tilde{1} = 0, \tilde{3} = 1$ ) and we are done. Thus summation

$\sum_{a \in G_a(0^{-1})} \left( \sum_{c \in G_a} A_{ca} \right)$  can be written as  $\sum_{a \in G_a(0^{-1})} \sum_{c \in G_a} (A_{ca} + A_{da})$ , where  $c$ 's and  $d$ 's have complementary

trace numbers. As 'a' spans whole of  $G_a(0^{-1})$ , 'ca' and 'da' span entire  $G_a$ . Thus from (3.2.12) the summation becomes  $2^{r-1}(J-I-E)$  as required. Now consider summation of second term in (3.2.16) over  $G_a(0^{-1})$ . Since  $\text{tr}(\tilde{\gamma}) = 0$ ,  $\text{tr}(\tilde{a}\tilde{\gamma})$  is also 0. Hence summations  $\sum A_a$  and  $\sum A_{a\gamma}$  over  $G_a(0^{-1})$  are equal. Taking the summation of first term in (3.2.16) as in the proof of Lemma 3.2.3 completes the proof of (3.2.14). Similar argument applies to (3.2.15) since  $\text{tr}(\tilde{\gamma}) = 0$ .  $\square$

### 3.3 Trace Sequence Families over $Z_{2^k}$

This section defines a family of sequences associated with any unit element  $\alpha$  belonging to  $\text{GR}(4, r)$  by making use of the trace function given in Appendix A. The sequences are generated as the trace of successive powers of  $\alpha$ ; the multiplicative order of  $\alpha$  determines the period of the sequences. Since  $Z_{2^k}$  is a local ring, any family of trace sequences over  $Z_{2^k}$  includes sequences over its ideals also. The sequences over the ideal isomorphic to  $Z_{2^\kappa}$ ,  $1 \leq \kappa < k$ , are denoted as  $(k-\kappa)^{\text{th}}$  level sequences, and accordingly, there are totally  $k$  level sequences. A  $\kappa^{\text{th}}$  level sequence associated with a unit element  $a \in G_a$  of  $\text{GR}^*(2^{k-\kappa}, r)$ ,

CENTRAL LIBRARY  
I. I. T. KANPUR

Acc. No. A. 116564 A 116564

$S^{\kappa, a} = \{s_i^{\kappa}\}$  (isomorphic to a sequence over  $Z_{2^k - \kappa}$ ) is given by  $s_i^{\kappa} = \text{tr}_1^r(2^{\kappa} a \alpha^i)$ ;  $i \in Z_L$ , where  $L$  is the period of  $\alpha$ . It is clear that the total number of sequences in the family is  $(2^{kr} - 1 / L)$ .

The trace sequence generated by an element  $\alpha$  satisfies a linear recursion over  $Z_{2^k}$ , given by  $s_j = - \sum_{i=0}^{r-1} c_i s_{j-r+i}$ ;  $c_i \in Z_{2^k}$ ,  $j = r, r+1, \dots$ . The corresponding connection polynomial  $C(d)$  is given by  $d^r + \sum_{i=0}^{r-1} c_i d^i$ , which is the minimum polynomial  $m_{\alpha}(d)$  of degree  $r$  over  $Z_{2^k}$ . Thus  $C(d) = m_{\alpha}(d) = (d - \alpha)(d - \sigma(\alpha)) \dots (d - \sigma^{r-1}(\alpha))$ .

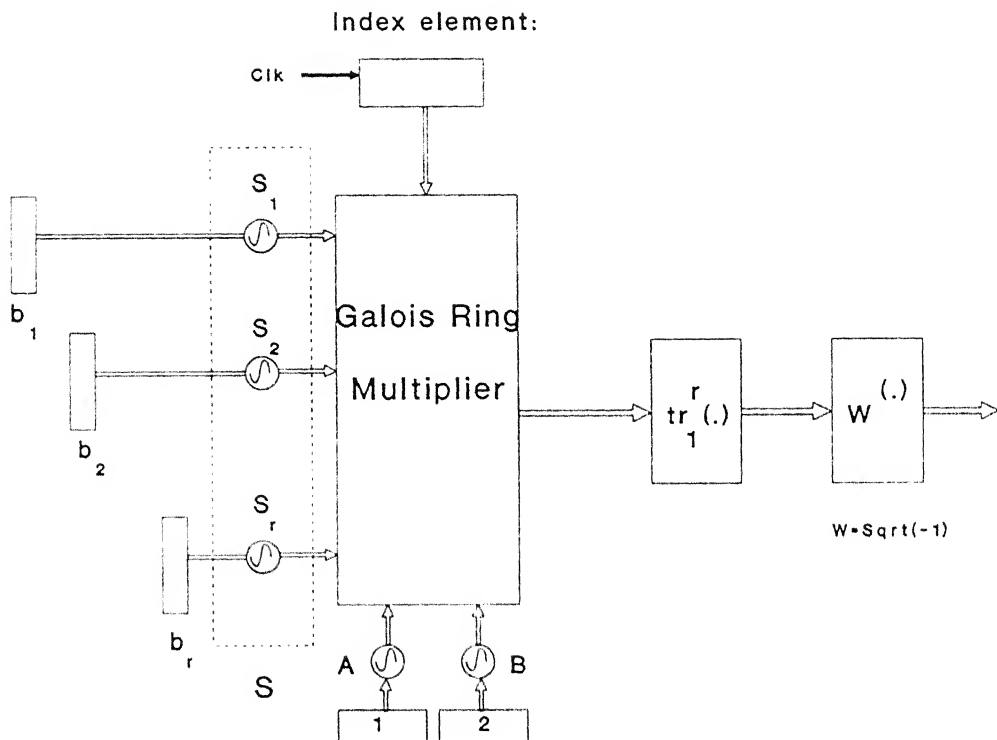
### 3.4 Families of Maximal-length Sequences over $Z_4$

This section deals with the ring  $Z_{2^k}$  when  $k = 1$ . If a primitive element,  $\alpha \in G_c$  is chosen for trace sequence generation, the resulting sequences are called maximal length sequences (m-sequences) over  $Z_4$ . A family of m-sequences over  $Z_4$  ( $\mathcal{K}$  family) is a collection of  $2^r + 1$  sequences, each of period  $2^r - 1$ . This class includes an m-sequence over  $Z_2$ , the binary field. An m-sequence associated with an element  $a$ ,  $S^a = \{s_i\}$ , is given by  $s_i = \text{tr}_1^r(a \alpha^i)$ ;  $i \in Z_{2^r - 1}$ . The distinct zeroth level sequences are given by the set  $\{S^a, a \in G_a\}$ , where  $G_a$  is the Abelian component group of  $\text{GR}^*(4, r)$ , which accounts for  $2^r$  sequences. Unique first level sequence  $S^2$  is isomorphic to a binary m-sequence. Schematic diagram of m-sequence generation over  $Z_4$  is given in Fig 3.4.1. For computing correlation properties of m-sequences, following definition is helpful.

**Definition 3.4.1:** Trace number of an m-sequence  $S^u$ : The trace number of a  $Z_4$  m-sequence  $S^u$ ;  $u \in \text{GR}^*(4, r)$ , is defined as the trace number of  $u$ .

#### 3.4.1 Number of Cyclically Equivalent Families

Two  $\mathcal{K}$  families are cyclically equivalent if the sequences of one family are obtained as cyclic shifts of sequences in the other. This is possible if and only if their linear recursions match. Two families  $\mathcal{K}^{\alpha_1}$  and  $\mathcal{K}^{\alpha_2}$  have same linear recursion if and only if  $\alpha_1$  is an automorphism of  $\alpha_2$ . Hence m-sequence families  $\mathcal{K}^{\sigma^i(\alpha)}$ ;  $i \in Z_r$ , are all cyclically equivalent. There are exactly  $\phi(2^r - 1)/r$  distinct  $\mathcal{K}$  families, where  $\phi$  is the Euler's  $\phi$  function.



S: Switch Board to select one of the  $2^r$  zero level sequences

$b_1, b_2, \dots, b_r$  : Basis elements of Standard Product

Representation of  $G_a$

Switch Arrangement

A	B	
Closed	Open	Zeroth level sequence
0	Closed	First level sequence

Fig 3.4.1 Schematic Diagram of m-sequence Generation over  $Z_4$

### 3.4.2 Correlation Computations of $m$ -sequences over $Z_4$

Analytical closed form expressions for correlation transform ( $\kappa$ ) of  $m$ -sequences over  $Z_4$  are derived in this section. The linearity property of  $m$ -sequences and the fact that the ring  $Z_4$  is a matched ring for quadriphase design, make the crosscorrelation computation of  $m$ -sequences equivalent to computation of  $\kappa$  of  $m$ -sequences. (Note that  $\kappa$  is a property of sequence, whereas, the crosscorrelation and autocorrelation values depend on  $\kappa$  of difference (point wise subtraction) of two sequences). Determining the  $\kappa$  of  $m$ -sequences is equivalent to finding the weight vectors associated with the sequences (See (3.4)). In the binary case, there is only one cyclically equivalent  $m$ -sequence, and hence, calculation of weight vector or  $\kappa$  does not pose a serious problem ( $\kappa$  of a binary  $m$ -sequence is  $-1$ ). But in this case, there are  $2^r+1$  sequences; and calculation of weight vectors or  $\kappa$ , at the outset, appears to be quite a formidable combinatorial task. Here a recourse into the theory of algebraic association schemes is taken for  $\kappa$  computations. We make use of the association scheme  $(GR(4,r),X)$  given in Section 3.2. In the sequel, it will be shown that  $\kappa$  of  $m$ -sequences are same as the eigenvalues of the adjacency matrices of the association scheme  $(GR(4,r),X)$ . The approach is similar to one used by Sole [31] for calculating correlation properties of  $m$ -sequences of period  $2^r-1$ ;  $r$  an odd integer.

*An Association Scheme over  $m$ -sequences:* A  $2^r+2$  class association scheme with a ground set  $Z_4$  is considered. Points of the scheme are all shifts of  $m$ -sequences, including the all zero sequence (points are all codewords of cyclic code  $(2^r-1,r,3)$  over  $Z_4$ ), which accounts for a total of  $4^r$  points. Each class consists of a cyclically distinct  $m$ -sequence and all its cyclic shifted versions. Two sequences are  $i^{\text{th}}$  associates if their difference belongs to  $i^{\text{th}}$  cyclically equivalent class. It is easy to verify that the scheme defined above is isomorphic to  $(GR(4,r),X)$  (Section 3.2). Thus, for the computation of intersection numbers of the scheme, it is advantageous to consider the scheme  $(GR(4,r),X)$ . Following theorem relates correlation transforms of  $m$ -sequences with eigenvalues of the scheme.

**Theorem 3.4.1:** The eigenvalues of the scheme  $(GR(4,r),X)$  are the correlation transforms of the  $m$ -sequences, and the eigenvalue distribution of adjacency matrices  $A_a$ ,  $a \in G_a$  gives the set of cross correlation values between an  $m$ -sequence,  $S^a$ , and all the phases of  $m$ -sequences including the all zero sequence.

**Proof:** First part of the theorem is readily obtained by substituting (3.2.5) for the eigenvalue expression in the Theorem 3.2.1 ((3.2.3)). By substituting (3.2.5) in (3.2.3), the  $z^{\text{th}}$  eigenvalue  $P_k(z)$  becomes



$$P_k(z) = \sum_{u \in [k]} \omega^{\text{tr}(uz)}, \quad (3.4.1)$$

which is equal to  $\aleph(S^{k*})$  as required from (2.1.7). The crosscorrelation values between a sequence  $S^a$  and all the cyclic shifts of sequences in the family including the all zero sequence  $S^0$ ; is given by the set:

$$\{C_{ab}(\tau), \tau \in Z_{2^r-1}, \text{ for all } b \in (\mathcal{K} \cup S^0)\}. \text{ Equivalently, from (2.1.11), it can be written as}$$

$$\{\aleph(S^a - T^l(B)), \tau \in Z_{2^r-1}, B \in (\mathcal{K} \cup S^0)\}, \quad (3.4.2)$$

where  $T^\tau$  represents  $\tau^{\text{th}}$  shift. Since  $\mathcal{K}$  is a linear family, cross correlation values belong to the set:

$$\{\aleph(T^l(B)), B \in (\mathcal{K} \cup 0)\} = \{\aleph(S^z), z \in \text{GR}(4, r)\}, \quad (3.4.3)$$

which is precisely the set of eigenvalues of  $A_a$ , where  $a$  is not a zero divisor.  $\square$

Thus a relation between the  $\aleph$  of the sequences and the eigenvalues of the scheme is established. Now it only remains to calculate the eigenvalues of adjacency matrices of B-M algebra with its multiplicities.

**Theorem 3.4.2:** The correlation transform values of all phases of  $(\mathcal{K} \cup S^0)$  is given in Table 3.4.1.

**Table 3.4.1**  
**Correlation Transform Distribution of All**  
**Phases of m-sequences over  $Z_4$  of Period  $2^r-1$**

$r = 2t+1$ an odd integer		$r = 2t$ an even integer	
$\aleph$	No of occurrences	$\aleph$	No of occurrences
$2^r-1$	1.	$2^r-1$	1.
$-1$	$(2^r-1).$	$-1$	$(2^r-1)$
$2^t-1 + \omega 2^t$	$2^{t-1}(2^t+1)(2^r-1).$	$2^t-1$	$2^{t-1}(2^{t-1}+1)(2^r-1).$
$-2^t-1 - \omega 2^t$	$2^{t-1}(2^t-1)(2^r-1).$	$-2^t-1$	$2^{t-1}(2^{t-1}-1)(2^r-1).$
$2^t-1 - \omega 2^t$	$2^{t-1}(2^t+1)(2^r-1).$	$-1 + \omega 2^t$	$2^{2t-2}(2^r-1).$
$-2^t-1 + \omega 2^t$	$2^{t-1}(2^t-1)(2^r-1).$	$-1 - \omega 2^t$	$2^{2t-2}(2^r-1).$

**Proof:** From the Theorem 3.4.1, it is sufficient to compute the spectrum of any incidence matrix  $A_a$ ,  $a$  is not a zero divisor. Spectrum computations are given below

*Case I ( $r$  odd,  $r = 2t+1$ ):*

Eigenvalues of  $E$ : If  $(a+\omega b)$  is an eigenvalue of  $A_a$ , then eigenvalue of  $A_{3a}$  is  $(a-\omega b)$ , since  $A_a^T = A_{3a}$ . Also since  $E^T = E$ , any eigenvalue of  $E$  can only be a real number. Then, from (3.2.7), we get  $a^2 = (2^r-1) + (2^r-2)a$ , which has solutions at  $a = -1$  or  $2^r-1$ .

Eigenvalues of  $A_a$ : Since  $[2a] = [e]$ ,  $A_a$  has  $-1$  as its eigenvalue with multiplicity  $2^r-1$ . Let  $\lambda = (a+\omega b)$  be an another eigenvalue of  $A_a$ , then from (3.2.9) we have

$$a^2 + b^2 + 2a = 2^r - 1. \quad (3.4.4)$$

Also, since  $r$  is odd, the trace numbers of  $a$  and  $3a$  are complimentary, and hence from (3.2.10) we have

$$\begin{aligned} A_a^2 + A_{3a}^2 &= 2E + 2 \sum_{a \neq b \neq 3a} A_b, \quad b \in G_c \\ &= 2(J - I) - 2(A_a + A_{3a}); \end{aligned} \quad (3.4.5)$$

where  $J = \sum A_a + I + E$  is the all 1 matrix of order  $4^r$ , and  $\bar{a}$  is the trace number of  $a$ . The above equation in terms of eigenvalues can be written as

$$2(a^2 - b^2) + 4a = -2. \quad (3.4.6)$$

The solution of (3.4.4) and (3.4.6) yields the result.

*Multiplicity calculations:* In all multiplicity calculations in this proof, the use of the relation  $\text{TRACE}(A_a) = 0$  is made, where  $\text{TRACE}(A)$  is the sum of all diagonal elements in  $A$ . The eigenvalue  $2^r-1$  occurs once and the eigenvalue of  $-1$  due to  $E$ , occurs  $2^r-1$  times. Let  $m_1$  and  $m_2$  be the multiplicities of eigenvalues  $2^t-1 + \omega 2^t$  and  $-2^t-1 + \omega 2^t$  respectively, then  $\text{TRACE}(A_a) = 0$  implies

$$(2^t-1) 2m_1 - (2^t+1) 2m_2 = 0, \text{ and } 2m_1 + 2m_2 = 4^r - 2^r,$$

solutions of which yield the result.

*Case II ( $r$  even,  $r = 2t$ ):*

Eigenvalues of  $E$  remain same as in the previous case.

Eigenvalues of  $A_a$ : Since  $r = 2t$ , trace numbers of  $a$  and  $3a$  are not complimentary and the (3.4.5) no longer holds. Thus, consider two adjacency matrices  $A_a$  and  $A_c$  such that trace numbers of  $a$  and  $c$  are

complementary. Then using (3.2.10) we can write

$$\begin{aligned} A_a^2 + A_c^2 &= 2E + 2 \sum_{a \neq b \neq c} A_b; b \in G_a \\ &= 2(J - I) - 2(A_a + A_c) \end{aligned} \quad (3.4.7)$$

where  $J = \sum A_a + I + E$ , the all 1 matrix of order  $4^r$ . Let  $\lambda_1 = (a + \omega b)$  and  $\lambda_2 = (c + \omega d)$  be eigenvalues of  $A_a$  and  $A_c$  respectively. Applying  $\lambda_1$  and  $\lambda_2$  in the above equation gives

$$a^2 + c^2 - b^2 - d^2 + 2a + 2c = -2, \quad (3.4.8)$$

$$2(ab + cd + b + d) = 0. \quad (3.4.9)$$

Also, applying  $\lambda_1$  and  $\lambda_2$  in (3.2.9) results

$$a^2 + b^2 + 2a = 2^r - 1. \quad (3.4.10)$$

$$c^2 + d^2 + 2c = 2^r - 1. \quad (3.4.11)$$

Simplifying (3.4.8), (3.4.10) and (3.4.11), we get  $b^2 + d^2 = 2^{2t}$ , this is possible if and only if  $b=0$  or  $d=0$  since  $b, d$ , and  $2^t$  form a Pythagorean triplet and  $b^2 + d^2 = 0 \pmod{4}$  [91]. Let  $b = 0$ , then  $d = \pm 2^t$ . Substituting these in (3.4.10) and (3.4.11) does the job.

**Multiplicity calculations:** In this case also,  $2^r - 1$  occurs once and  $-1$  occurs  $2^r - 1$  times. Let  $m_1, m_2, m_3$  be multiplicities of eigenvalues  $2^t - 1, -(2^t + 1), (-1 \pm \omega 2^t)$  respectively.  $\text{TRACE}(A_a) = 0$  implies  $(2^t - 1)m_1 - (2^t + 1)m_2 - 2m_3 = 0$ , and  $m_1 + m_2 + 2m_3 = 4^r - 2^r$ .

From (3.4.1) and (3.4.3), the eigenvalues of  $A_a$  are given by the set  $\{\aleph(S^{az}), z \in \text{GR}(4, r)\}$ . Also it is easy to see that all  $S^z$  with  $\aleph$  value  $(-1 \pm \omega 2^t)$  have the same trace number. If not, there exist two sequences of different trace numbers,  $S^a$  and  $S^c$  having the same  $\aleph$  value as  $(-1 \pm \omega 2^t)$ . Then applying this in (3.4.7) results in contradiction. There are exactly  $2^{r-1}(2^r - 1)$  sequences  $S^z$  which have the same trace number. Hence  $2m_3 = 2^{r-1}(2^r - 1)$ . Applying this in previous equations yields the result.  $\square$

Theorem 3.4.2 gives  $\aleph$ 's of all  $2^r - 1$  phases of  $m$ -sequences. But to get  $\aleph$  transform distribution, these  $2^r - 1$  phases need to be divided from the multiplicities given in the Table 3.4.1. Also note that the sequences in any subsets have a unique trace number. The tables of  $\aleph$  and the weight distributions with trace numbers are given in the following theorem. They are given explicitly here since they are used in subsequent sections repeatedly.

**Theorem 3.4.3:** The  $\aleph$  and Weight distributions of  $m$ -sequences over  $Z_4$  of period  $2^r-1$  are given in Table 3.4.2. The trace numbers of sequences within any subset are same. Also subsets  $\mathcal{P}$ ,  $\mathcal{Q}$  are called as complementary subsets to subsets  $\mathcal{R}$ ,  $\mathcal{S}$  respectively and vice versa, since, trace numbers associated with them are complementary to each other. For items 2 to 5,  $w_1 = 2^{r-1} - w_0$  and  $w_2 = 2^{r-1} - w_0$ . For the item 1 (corresponding to binary  $m$ -sequence),  $w_2 = 2^{r-1}$ , and  $w_3 = 0$ .

Table 3.4.2

Correlation Transform and Weight Distributions of  $m$ -sequences of Period  $2^r-1$

(a)  $r$ : odd integer,  $r = 2t+1$

Sl. No.	SUBSET	$\aleph$	No of seq' in the SUBSET	Trace Number	$w_0$	$w_1$
1.	binary	-1	1.	0	$2^{r-1}-1$	0
2.	$\mathcal{P}$	$2^t-1 + \omega 2^t$	$2^{t-1}(2^t+1)$	$\xi$	$2^{r-2}+2^{t-1}-1$	$2^{r-2}+2^{t-1}$
3.	$\mathcal{Q}$	$-2^t-1 - \omega 2^t$	$2^{t-1}(2^t-1)$	$\xi$	$2^{r-2}-2^{t-1}-1$	$2^{r-2}-2^{t-1}$
4.	$\mathcal{R}$	$2^t-1 - \omega 2^t$	$2^{t-1}(2^t+1)$	$\bar{\xi}$	$2^{r-2}+2^{t-1}-1$	$2^{r-2}-2^{t-1}$
5.	$\mathcal{S}$	$-2^t-1 + \omega 2^t$	$2^{t-1}(2^t-1)$	$\bar{\xi}$	$2^{r-2}-2^{t-1}-1$	$2^{r-2}+2^{t-1}$

(b)  $r$ : even integer,  $r = 2t$

Sl. No.	SUBSET	$\aleph$	No of seq' in the SUBSET	Trace Number	$w_0$	$w_1$
1.	binary	-1	1.	0	$2^{r-1}-1$	0
2.	$\mathcal{P}$	$2^t-1$	$2^{t-1}(2^{t-1}+1)$	$\xi$	$2^{r-2}+2^{t-1}-1$	$2^{r-2}$
3.	$\mathcal{Q}$	$-2^t-1$	$2^{t-1}(2^{t-1}-1)$	$\xi$	$2^{r-2}-2^{t-1}-1$	$2^{r-2}$
4.	$\mathcal{R}$	$-1 + \omega 2^t$	$2^{r-2}$	$\bar{\xi}$	$2^{r-2}-1$	$2^{r-2}+2^{t-1}$
5.	$\mathcal{S}$	$-1 - \omega 2^t$	$2^{r-2}$	$\bar{\xi}$	$2^{r-2}-1$	$2^{r-2}-2^{t-1}$

where  $\xi$  is the trace number of sequences in the subset and  $\bar{\xi}$  is complement of  $\xi$ .

**Proof:** It is easy to show that  $m$ -sequences in any subset have same trace number. If not it leads to a contradiction of (3.4.7). Also in a similar way one can show that subset  $\mathcal{P} \cup \mathcal{Z}$  has sequences with same trace number ( $\xi$ ) and subset  $\mathcal{Z} \cup \mathcal{R}$  has sequences with trace number complement to that of trace number of  $\mathcal{P} \cup \mathcal{Z}$ . Weight distribution is computed as follows. We have from (2.1.9), for any  $S^a$ ,  $\mathcal{K}(S^a) = (w_0 - w_2) + \omega(w_1 - w_3)$ , and thus differences  $(w_0 - w_2)$  and  $(w_1 - w_3)$  are known from the  $\mathcal{K}$  distribution. Also, the homomorphic mapping from  $Z_4$  to  $Z_2$  ( $\wedge$ ) takes  $S^a$  to a binary  $m$ -sequence which has number of zeros one less than number of one's. Under this mapping, elements 1 and 3 are mapped into 1, and, 2 and 0 are mapped into 0. Thus  $w_0 + w_2 = 2^{r-1} - 1$  and  $w_1 + w_3 = 2^{r-1}$ . Then by solving the above equations,  $w_i$ 's,  $i \in Z_4$  are computed. Only  $w_0$  and  $w_1$  is listed in the table for the rest is readily obtained from the above equations.  $\square$

*Example 3.4.1:*  $m$ -sequences of period  $L = 7$  generated by  $\alpha \in G_c$  of  $GR^*(4,3)$ , such that  $1 + 3\alpha + 2\alpha^2 = \alpha^3$ , are given in Table 3.4.3. The minimum polynomial  $m_\alpha(d)$  is  $(3 + d + 2d^2 + d^3)$ .

Table 3.4.3  $m$ -sequences of Period 7 (Example 3.4.1)

Sl. No	(a)	Sequence: $S^{\mathcal{K}}(S^a)$ =correlation transform	
1	(1)	2 2 1 2 1 1 3	$-3 + \omega 2$
2	(3)	2 2 3 2 3 3 1	$-3 - \omega 2$
3	$(1 + 2\alpha)$	2 0 1 0 3 3 3	$1 - \omega 2$
4	$(3 + 2\alpha)$	2 0 3 0 1 1 1	$1 + \omega 2$
5	$(1 + 2\alpha^2)$	0 2 3 0 3 1 3	$1 - \omega 2$
6	$(3 + 2\alpha^2)$	0 2 1 0 1 3 1	$1 + \omega 2$
7	$(1 + 2\alpha + 2\alpha^2)$	0 0 3 2 1 3 3	$1 - \omega 2$
8	$(3 + 2\alpha + 2\alpha^2)$	0 0 1 2 3 1 1	$1 + \omega 2$
9	(2)	0 0 2 0 2 2 2	$-1$

*Example 3.4.2:*  $m$ -sequences of period  $L=15$  generated by  $\alpha \in G_c$  of  $GR^*(4,4)$ , such that  $3 + \alpha + 2\alpha^2 = \alpha^4$ , are given in Table 3.4.4. The minimum polynomial  $m_\alpha(d)$  is  $(1 + 3d + 2d^2 + d^4)$ .

Table 3.4.4 m-sequences of Period 15 (Example 3.4.2)  
Elements of  $GR(4,r)$  is represented as 4 tuples over  $Z_4$

SL No	a	$S^a$	$\aleph(S^a)$
1	(1000)	003023103213110	3
2	(3000)	001021301231330	3
3	(1200)	023001123031310	3
4	(3200)	021003321013130	3
5	(1020)	203203301031110	3
6	(3020)	201201103013330	3
7	(1220)	223221321213310	-5
8	(3220)	221223123231130	-5
9	(1002)	001221121033112	$-1+\omega 4$
10	(3002)	003223323011332	$-1-\omega 4$
11	(1202)	021203101211312	$-1+\omega 4$
12	(3202)	023201303233132	$-1-\omega 4$
13	(1022)	201001323211112	$-1+\omega 4$
14	(3022)	203003121233332	$-1-\omega 4$
15	(1222)	221023303033312	$-1-\omega 4$
16	(3222)	223021101011132	$-1+\omega 4$
17	(2000)	002002202022220	-1

We need the following theorem for later use.

**Theorem 3.4.4:** The following results concerning the correlation transforms of m-sequences are true:

$$\sum_{a \in G_a} \aleph(S^a) = 0 \quad (3.4.12)$$

$$\sum_{a \in G_a} \aleph(S^a) \aleph(S^{a\gamma}) = -2^r \quad (3.4.13)$$

$$\sum_{S^a \in \mathcal{P} \cup \mathcal{L}} \aleph(S^a) \aleph(S^{a\gamma}) = -2^{r-1} - \omega(2^r), \text{tr}(\tilde{\gamma}) = 0, r:\text{odd} \quad (3.4.14)$$

$$\sum_{S^a \in \mathcal{P} \cup \mathcal{L}} \aleph(S^a) \aleph(S^{a\gamma}) = -3 \cdot 2^{r-1}, \text{tr}(\tilde{\gamma}) = 0, r:\text{even} \quad (3.4.15)$$

where  $\gamma \neq 1, 3$ .

**Proof:** (3.4.12) and (3.4.13) are obtained by applying  $\aleph(S^a)$  in Lemma 3.2.3 as equations on the adjacency matrices of the B-M algebra are also satisfied by their eigenvalues ( $\aleph(S^a)$  is an eigenvalue of  $A_a$ ). To prove (3.4.14) we observe that sequences in subset  $(\mathcal{P} \cup \mathcal{L})$  have same trace number  $\xi$ ,  $\xi$  is either 0 or 1. In any case (3.2.14) or (3.2.15) is applicable. Applying  $\aleph(S^a)$  in (3.2.14) or (3.2.15) we get

$$\sum_{a \in G_a(\xi^{-1})} \aleph(S^a) \aleph(S^{a\gamma}) = \sum_{S^a \in \mathcal{P} \cup \mathcal{L}} \aleph(S^a) \aleph(S^{a\gamma}) = -2^{r-1} - 2 \sum_{S^a \in \mathcal{P} \cup \mathcal{L}} \aleph(S^a). \text{ From Table 3.4.2 the}$$

summation  $\sum \aleph(S^a)$  over  $\mathcal{P} \cup \mathcal{L}$  is given by  $(2^t-1 + \omega 2^t) 2^{t-1}(2^t+1) + (-2^t-1 - \omega 2^t) 2^{t-1}(2^t-1)$ .

Simplification of this equation leads to (3.4.14). Similarly (3.4.15) can be proved.  $\square$ .

### 3.4.3 Correlation Distribution

Correlation distribution of  $\mathcal{K}$  is a collection of correlation values given by the set

$$\{C_{ab}(\tau), \text{ for all } a, b \in \mathcal{K}, \tau \in Z_{2^r-1}\} \quad (3.4.16)$$

From (2.1.11), this set can be equivalently expressed as  $\{\kappa(S^a - S^b) = \kappa(S^{a-b}), \text{ for all } a \in (G_a \cup S^2) \text{ and } b \in \text{GR}(4, r) \setminus \{0\}\}$ , where  $\setminus$  represents set theoretic subtraction. Since  $\mathcal{K}$  is a linear family, for a fixed  $S^a \in \mathcal{K}$ , the set  $\{\kappa(S^a - S^b), b \in \text{GR}(4, r) \setminus \{0\}\}$  covers  $\kappa$  of all phases of sequences in  $(\mathcal{K} \cup S^0)$  except  $S^a$ .

Thus, the set (3.4.16) can be written as

$$\{\kappa(S^0)\}^{2^r+1} \cup (\{\kappa(S^b); b \in \mathcal{K} \cup S^2\}^{(2^r+1)(2^r-1)} \setminus \{\kappa(S^a); a \in G_a \cup S^2\}),$$

where the numbers in the superscripts indicate the number of occurrences. The distribution of values in the set  $\{\kappa(S^a); a \in G_a \cup S^2\}$  is given in Theorem 3.4.3. Hence the correlation distribution is obtained by multiplying  $(2^r-1)(2^r+1) - 1 = 4^r - 2$  to all values in the 'no of occurrences' column of Table 3.4.2. An entry of  $\kappa(S^0) = 2^r - 1$  which occurs  $2^r + 1$  times needs to be added. The crosscorrelation distribution is given in Table 3.4.5.

Table 3.4.5 Crosscorrelation Distribution of  $\mathcal{K}$

r : odd integer, r = 2t+1		r : even integer, r = 2t	
$\kappa$	No of occurrences	$\kappa$	No of occurrences
$2^r - 1$	$2^r + 1.$	$2^r - 1$	$2^r + 1.$
-1	$(4^r - 2).$	-1	$(4^r - 2)$
$2^t - 1 + \omega 2^t$	$2^{t-1}(2^t + 1)(4^r - 2).$	$2^t - 1$	$2^{t-1}(2^{t-1} + 1)(4^r - 2).$
$-2^t - 1 - \omega 2^t$	$2^{t-1}(2^t - 1)(4^r - 2).$	$-2^t - 1$	$2^{t-1}(2^{t-1} - 1)(4^r - 2).$
$2^t - 1 - \omega 2^t$	$2^{t-1}(2^t + 1)(4^r - 2).$	$-1 + \omega 2^t$	$2^{2t-2}(4^r - 2).$
$-2^t - 1 + \omega 2^t$	$2^{t-1}(2^t - 1)(4^r - 2).$	$-1 - \omega 2^t$	$2^{2t-2}(4^r - 2).$

### 3.5 Families of Interleaved m-sequences

If an element  $\gamma\alpha$ ;  $\gamma \in G_a$  and  $\alpha$  primitive element in  $G_c$ , is used in the trace sequence generation method described in Section 3.3, the resulting sequences are of period  $2(2^r - 1)$ . A zeroth level sequence

associated with a unit element  $a$ ,  $IS^a = \{s_i\}$ , is given by  $s_i = \text{tr}_1^r(a(\gamma\alpha)^i)$ ,  $i \in Z_{2(2^r-1)}$ . Since  $\gamma^2 = 1$ , even index sequence bits are from  $m$ -sequence  $S^a$  and odd index bits are from  $m$ -sequence  $S^a\gamma\alpha$ .

$$s_{2i} = \text{tr}_1^r(a(\alpha^2)^i) = S_1^a, i^{\text{th}} \text{ bit of } S^a \quad (3.5.1)$$

$$s_{2i+1} = \text{tr}_1^r(a\gamma\alpha(\alpha^2)^i) = S_1^a\gamma\alpha; 0 \leq i < 2^{r-1}. \quad (3.5.2)$$

Hence these sequences are called as Interleaved  $m$ -sequences ( $\mathcal{IM}$ ). For each  $\gamma \in G_a$ , a distinct family of interleaved  $m$ -sequences,  $\mathcal{IM}^\gamma$  can be defined. It is clear that there are  $2^{r-1}$  zero-level sequences and are given by the set  $\{IS^a, a \in \text{Quotient group } G_a/(1, \gamma)\}$ . The elements in the quotient group  $G_a/(1, \gamma)$  are generated using a product representation of  $G_a$ . Find  $\beta_1, \beta_2, \dots, \beta_{r-1} \in G_a$  such that  $G_a = (1, \gamma) * (1, \beta_1) * \dots * (1, \beta_{r-1})$  where  $*$  denotes direct product notation. Construction of product representations is given in Section 3.1. Then the elements of  $G_a/(1, \gamma)$  are given by

$$a_i = (\beta_1)^{i_1}(\beta_2)^{i_2} \dots (\beta_{r-1})^{i_{r-1}}; i = i_1 + 2i_2 + \dots + 2^{r-2}i_{r-1}, \quad (3.5.3)$$

where  $i_k = 0$  or  $1$ ,  $k = 1, \dots, r-1$ . A first level  $\text{Im}$ -sequence,  $IS^2$ , is a binary  $m$ -sequence of period  $2^r-1$ .

*Generation of Im-sequences:* The schematic diagram of  $\text{Im}$ -sequence generation is same as that of  $\mathcal{M}$  except here, index element for sequence generation is  $(\gamma\alpha)$ , and, the standard product basis elements of  $G_a$  used for sequence selection in schematic diagram of  $\mathcal{M}$ , is replaced by a product representation of the quotient group  $G_a/(1, \gamma)$ . In this case, there are only  $r-1$  product basis elements which selects one of the  $2^{r-1}$   $\text{Im}$ -sequences.

### 3.5.1 Number of Distinct Families

There are  $2^r$   $\mathcal{IM}$  families corresponding to each  $\alpha \in G_c$ . Excluding a family corresponding to  $\gamma = 1$ , which is  $\mathcal{M}$ , a family of  $m$ -sequences, there are  $2^r-1$  proper  $\mathcal{IM}$  families. Moreover, there are  $N_2(r)$  distinct primitive elements in  $G_c$ , where  $N_2(r)$  is the number of primitive polynomials of degree  $r$ . Hence the total number of proper distinct  $\mathcal{IM}$  families is given by

$$N_{\text{Im-sequences}} = (2^r-1) * N_2(r) \quad (3.5.4)$$

### 3.5.2 Correlation Computation

The  $\mathcal{K}$  of  $\text{Im}$ -sequences are closely related to  $\mathcal{K}$  of constituent  $m$ -sequences. Let  $IS^a \in \mathcal{IM}^\gamma$ , then  $\mathcal{K}$  of  $IS^a$  is given by



$$\Re(IS^a) = \Re(S^a) + \Re(S^{a\gamma}) \quad (3.5.5a)$$

where  $S^a$  and  $S^{a\gamma}$  are the constituent  $m$ -sequences of  $IS^a$ . Similarly weight vector of a  $IS^a$  is given by

$$W(IS^a) = W(S^a) + W(S^{a\gamma}) \quad (3.5.5b)$$

We have the following lemma for the crosscorrelation between any two  $Im$ -sequences.

**Lemma 3.5.1:** Let  $X$  and  $Y$  be two complex valued sequences of period  $2(2^r-1)$  derived from  $Im$ -sequences  $IS^a$  and  $IS^b$  respectively. Then, the crosscorrelation between  $X$  and  $Y$  is given by  $C_{XY}(\tau) = \Re(S^\eta) + \Re(S^{\eta\gamma})$ , where  $\eta = (a - b(\gamma\alpha)^\tau)$  (3.5.6)

**Proof:** From (2.1.11), the crosscorrelation between  $X$  and  $Y$ ,  $C_{XY}(\tau)$ , is given by  $\Re(IS^a - T^\tau(IS^b))$  which is equal to  $\Re(IS^a - IS^{b(\gamma\alpha)^\tau})$ . Using (3.5.1) and (3.5.2), this can be expressed as  $\Re(S^a - S^{b(\gamma\alpha)^\tau}) + \Re(S^{a\gamma\alpha} - S^{b(\gamma\alpha)^{\tau+1}})$  which is equal to  $\Re(S^\eta) + \Re(S^{\eta\gamma\alpha})$  as required.  $\square$

From the above it is clear that the crosscorrelation between any two  $Im$ -sequences is always a sum of  $\Re$  of two  $m$ -sequences. At the outset it appears that  $\theta_{\max}$  for  $\mathcal{JK}$  families is twice that of  $\mathcal{K}$  families. But, for some suitable choice of  $\gamma$ ,  $\theta_{\max}$  can be bounded to the Welch limit by making use of specific nature of  $\Re$  values of  $m$ -sequences. In the following, the  $\Re$  distribution of  $\mathcal{JK}$ -families is computed.

From (3.5.5a)  $\Re$  of  $Im$ -sequence  $IS^a$  is the sum of  $\Re$  of two  $m$ -sequences  $S^a$  and  $S^{a\gamma}$ . The elements  $a$  and  $\gamma$  can be expressed as  $a = 1+2\bar{a}$ ,  $\gamma = 1+2\bar{\gamma} \in G_a$ , and thus  $a\gamma = 1+2(\bar{a}+\bar{\gamma})$ , where  $\bar{\cdot}$  represents the isomorphism between  $G_a$  and  $GF(2^r)$ . Now, if the trace number of  $a$ ,  $\text{tr}(\bar{a})$ , is  $\xi$  then the trace number of  $a\gamma$  is  $\xi + \text{tr}(\bar{\gamma})$ . Thus the trace numbers of constituent  $m$ -sequences of a family,  $\mathcal{JK}^\gamma$ , are related through the trace number of  $\gamma$ , and correspondingly,  $\mathcal{JK}$  families are grouped under the following categories.

Category 1: Families  $\mathcal{JK}^\gamma$  such that  $\text{tr}(\bar{\gamma}) = 1$ ,  $\gamma = (1+2\bar{\gamma})$ :  $\mathcal{JK}^\gamma(\text{tr}(\bar{\gamma})=1)$

Category 2: Families  $\mathcal{JK}^\gamma$  such that  $\text{tr}(\bar{\gamma}) = 0$ ,  $\gamma = (1+2\bar{\gamma})$ :  $\mathcal{JK}^\gamma(\text{tr}(\bar{\gamma})=0)$

Category 3: Family  $\mathcal{JK}^\gamma$  such that  $\gamma = 3$ :  $\mathcal{JK}^\gamma(\gamma = 3)$

The family  $\mathcal{JK}^3$  is considered as a separate category, since the trace number of 3 is 1 when  $r$  is odd and 0 when it is even. If the  $\text{tr}(\bar{\gamma})$  is 0, then  $\Re(S^a)$  and  $\Re(S^{a\gamma})$  belongs to the subsets with same trace number and if  $\text{tr}(\bar{\gamma})$  is 1, then  $\Re(S^a)$  and  $\Re(S^{a\gamma})$  belongs to the subsets with different trace numbers. From

Theorem 3.4.3, sequences in the subsets  $\mathcal{P}$  and  $\mathcal{L}$  have same trace number  $\xi$  and those in subsets  $\mathcal{R}$  and  $\mathcal{S}$  have a trace number  $\bar{\xi}$ , compliment of  $\xi$ . Consequently, if  $\text{tr}(\bar{\gamma})$  is 1, both the constituent sequences can not belong to  $(\mathcal{P} \cup \mathcal{L})$  or  $(\mathcal{R} \cup \mathcal{S})$ ; ie. in  $\text{IS}^a$ , if  $S^a \in (\mathcal{P} \cup \mathcal{L})$ , then necessarily  $S^{a\gamma} \in (\mathcal{R} \cup \mathcal{S})$ . For a notational sake, the constituent sequences of an Im-sequence  $\text{IS}^a$ ,  $S^a$  and  $S^{a\gamma}$ , are called as associates; and if  $S^a \in \mathcal{P}$ ,  $S^{a\gamma} \in \mathcal{R}$ , this association is represented by  $(\mathcal{P} \& \mathcal{R})$ . Thus, if  $\text{tr}(\bar{\gamma})$  is 1, the possible associations for constituent sequences of Im-sequences, are of types  $(\mathcal{P} \& \mathcal{R})$ ,  $(\mathcal{P} \& \mathcal{S})$ ,  $(\mathcal{L} \& \mathcal{R})$ ,  $(\mathcal{L} \& \mathcal{S})$ . Similarly if  $\text{tr}(\bar{\gamma})$  is 0, both the constituent sequences belong to either  $(\mathcal{P} \cup \mathcal{L})$  or  $(\mathcal{R} \cup \mathcal{S})$  and the possible associations are  $(\mathcal{P} \& \mathcal{P})$ ,  $(\mathcal{L} \& \mathcal{L})$ ,  $(\mathcal{P} \& \mathcal{L})$ ,  $(\mathcal{R} \& \mathcal{R})$ ,  $(\mathcal{S} \& \mathcal{S})$ ,  $(\mathcal{R} \& \mathcal{S})$ . Thus  $\aleph$  values, weight vectors of Im-sequences can be computed and subsets having common  $\aleph$  value can be tabulated. Now it only remains to compute the number of sequences which have the same association.

We shall first consider the case of  $\gamma = 3$ , where the computation is relatively simple. In this case  $\aleph$  of constituent sequences are complex conjugate of each other, since, if  $\aleph(S^a) = a + \omega b$ ,  $\aleph(S^{3a}) = a - \omega b$ . When  $r$  is odd,  $\text{tr}(\bar{3}) = 1$ , and all the sequences in  $\mathcal{P}$  and  $\mathcal{L}$  is associated with sequences in  $\mathcal{R}$  and  $\mathcal{S}$  respectively, since  $\aleph$  of sequences in  $\mathcal{P}$  and  $\mathcal{R}$ , and of sequences in  $\mathcal{L}$  and  $\mathcal{S}$  are conjugate of each other (Table 3.4.2). Hence there are only two subsets  $\mathcal{P}$ ,  $\mathcal{L}$  in  $\aleph$  distribution of  $\mathcal{MK}(\gamma=3)$ , whose constituent associations are  $(\mathcal{P} \& \mathcal{R})$  and  $(\mathcal{L} \& \mathcal{S})$  respectively, and  $|\mathcal{P}| = |\mathcal{P}|$  and  $|\mathcal{L}| = |\mathcal{L}|$ , where  $|x|$  represents the cardinality of  $x$ . Similarly, when  $r$  is even,  $\text{tr}(\bar{3})$  is 0 and we have three subsets  $\mathcal{P}$ ,  $\mathcal{L}$ ,  $\mathcal{R}$  whose constituent associations are  $(\mathcal{P} \& \mathcal{P})$ ,  $(\mathcal{L} \& \mathcal{L})$  and  $(\mathcal{R} \& \mathcal{S})$  respectively. Thus we have  $|\mathcal{P}| = |\mathcal{P}|/2$ ,  $|\mathcal{L}| = |\mathcal{L}|/2$ ,  $|\mathcal{R}| = |\mathcal{R}|$ . This way, the cardinalities of the subsets are computed and the results are tabulated in Table 3.5.3. When  $\gamma \neq 3$ , the computation of distributions is not straight forward. We need the following lemma.

**Lemma: 3.5.2:** The following results concerning the correlation transforms of Im-sequences are true:

$$\sum_{a \in G_a / \{1, \gamma\}} \aleph(\text{IS}^a) = 0 \quad (3.5.7)$$

$$\sum_{a \in G_a / \{1, \gamma\}} \aleph(S^a) \aleph(S^{a\gamma}) = -2^{r-1} \quad (3.5.8)$$

where  $S^a, S^{a\gamma}$  are the constituent m-sequences of Im-sequences.

**Proof:** From (3.5.5a), the LHS of (3.5.7) can be written as

$$\sum_{a \in G_a / \{1, \gamma\}} \aleph(\text{IS}^a) = \sum_{a \in G_a / \{1, \gamma\}} \aleph(S^a) + \aleph(S^{a\gamma}) = \sum_{a \in G_a} \aleph(S^a), \text{ which is equal to zero from (3.4.12). To}$$

prove (3.5.8), consider (3.4.13),  $\sum_{a \in G_a} \kappa(S^a) \kappa(S^a \gamma) = -2^r$ . The LHS of this equation can be split up into two summands given by  $\sum_{a \in G_a / \{1, \gamma\}} \kappa(S^a) \kappa(S^a \gamma) + \sum_{a \in \gamma(G_a / \{1, \gamma\})} \kappa(S^a) \kappa(S^a \gamma)$ , which can be simplified as  $\sum_{a \in G_a / \{1, \gamma\}} \kappa(S^a) \kappa(S^a \gamma) + \sum_{a \in (G_a / \{1, \gamma\})} \kappa(S^a \gamma) \kappa(S^a)$ , which in turn equal to  $2 \sum_{a \in G_a / \{1, \gamma\}} \kappa(S^a) \kappa(S^a \gamma)$ . Then dividing 2 from both sides gives the desired result.  $\square$

Case 1 ( $\text{tr}(\bar{\gamma}) = 1$ ):

From Table 3.4.2, it is seen that Im-sequences with associations  $(\mathcal{P} \& \mathcal{R})$ ,  $(\mathcal{P} \& \mathcal{S})$ ,  $(\mathcal{Z} \& \mathcal{R})$ ,  $(\mathcal{Z} \& \mathcal{S})$  give rise to distinct  $\kappa$  values and subsets with these associations are correspondingly named as  $\mathcal{P}$ ,  $\mathcal{Z}$ ,  $\mathcal{R}$ ,  $\mathcal{S}$ . The problem here is to compute cardinalities of these subsets. Since there are  $2^{r-1}$  Im-sequences in any family, volume constraint implies

$$|\mathcal{P}| + |\mathcal{Z}| + |\mathcal{R}| + |\mathcal{S}| = 2^{r-1}$$

When  $r$  is odd,  $\kappa$  value and the product of  $\kappa$  values of constituent m-sequences, of Im-sequences in the subsets  $\mathcal{P}$ ,  $\mathcal{Z}$ ,  $\mathcal{R}$ ,  $\mathcal{S}$  are as follows

Subsets	Association	$\kappa(\text{IS}^a)$	$\kappa(S^a)\kappa(S^a \gamma)$
$\mathcal{P}$	$(\mathcal{P} \& \mathcal{R})$	$2(2^t - 1)$	$2^{2t+1} - 2^{t+1} + 1$
$\mathcal{Z}$	$(\mathcal{Z} \& \mathcal{S})$	$-2(2^t + 1)$	$2^{2t+1} + 2^{t+1} + 1$
$\mathcal{R}$	$(\mathcal{P} \& \mathcal{S})$	$-2 + \omega 2^{t+1}$	$-2^{2t+1} + 1 - \omega 2^{t+1} + 1$
$\mathcal{S}$	$(\mathcal{Z} \& \mathcal{R})$	$-2 - \omega 2^{t+1}$	$-2^{2t+1} + 1 + \omega 2^{t+1} + 1$

Relation  $|\mathcal{R}| = |\mathcal{S}|$ , is seen easily since any  $\text{IS}^a \in \mathcal{R}$  implies  $\text{IS}^{3a} \in \mathcal{S}$  and thus subsets  $\mathcal{R}$  and  $\mathcal{S}$  have same number of sequences (Symmetry argument). Now applying these results in (3.5.7) and (3.5.8) yields

$$2^t(|\mathcal{P}| - |\mathcal{Z}|) = 2^{r-1}$$

$$|\mathcal{P}| + |\mathcal{Z}| = |\mathcal{R}| + |\mathcal{S}| = 2|\mathcal{R}| = 2^{r-2}.$$

When  $r$  is even,  $\kappa$  values of  $\mathcal{P}$  and  $\mathcal{R}$ , and of  $\mathcal{Z}$  and  $\mathcal{S}$ , are conjugate of each other. Thus by the symmetry argument,  $|\mathcal{P}| = |\mathcal{R}|$  and  $|\mathcal{Z}| = |\mathcal{S}|$ , which then by using volume constraint implies

$$|\mathcal{P}| + |\mathcal{Z}| = |\mathcal{R}| + |\mathcal{S}| = 2^{r-2}.$$

From (3.5.7) we have

$$2^t(|\mathcal{P}| - |\mathcal{Z}|) = 2^{r-1}.$$

Solving the above equations, for both the cases when  $r$  is odd and even, the cardinality of the subsets  $\overline{\mathcal{P}}, \overline{\mathcal{Z}}, \overline{\mathcal{R}}, \overline{\mathcal{S}}$  are computed and the results are tabulated in Table 3.5.1.

*Case 2* ( $\text{tr}(\tilde{\gamma}) = 0$ ):

In this case, there are five modified subsets having common  $\aleph$  values; they are, with their constituent associations, given by  $\overline{\mathcal{P}} = (\mathcal{P} \& \mathcal{A})$ ,  $\overline{\mathcal{Z}} = (\mathcal{Z} \& \mathcal{Z})$ ,  $\overline{\mathcal{R}} = (\mathcal{R} \& \mathcal{R})$ ,  $\overline{\mathcal{S}} = (\mathcal{S} \& \mathcal{S})$ , and a subset  $\mathcal{Z}_1 \cup \mathcal{Z}_2 \{ \mathcal{Z}_1 = (\mathcal{P} \& \mathcal{Z}) \mathcal{Z}_2 = (\mathcal{R} \& \mathcal{S}) \}$ , where  $\cup$  represents set theoretic union. Again, the volume constraint implies

$$|\overline{\mathcal{P}}| + |\overline{\mathcal{Z}}| + |\overline{\mathcal{R}}| + |\overline{\mathcal{S}}| + (|\mathcal{Z}_1| + |\mathcal{Z}_2|) = 2^{r-1}. \quad (3.5.9)$$

Also constituent sequences of Im-sequences in the subset  $\overline{\mathcal{P}} \cup \overline{\mathcal{Z}} \cup \mathcal{Z}_1$  accounts for all  $m$ -sequences from the subset  $\mathcal{P} \cup \mathcal{Z}$  whose size is  $2^{r-1}$ . This along with (3.5.9) then implies

$$|\overline{\mathcal{P}}| + |\overline{\mathcal{Z}}| + |\mathcal{Z}_1| = 2^{r-2} = |\overline{\mathcal{R}}| + |\overline{\mathcal{S}}| + (|\mathcal{Z}_2|) \quad (3.5.10)$$

Arguments for cardinality computations of subsets runs similar to the previous case, except here we have to make use of (3.4.14) and (3.4.15). Lemma 3.5.3 is useful for calculating cardinalities.

**Lemma 3.5.3:** For  $\gamma \neq 1, 3$  with  $\text{tr}(\tilde{\gamma}) = 0$ ,

$$\sum \aleph(S^a) \aleph(S^{a\gamma}) = -2^{r-2} - \omega(2^{r-1}); \quad r:\text{odd} \quad (3.5.11)$$

$$\sum \aleph(S^a) \aleph(S^{a\gamma}) = -3 \cdot 2^{r-2}; \quad r:\text{even} \quad (3.5.12)$$

where summation is carried over all Im-sequences  $IS^a$  in the subset  $(\overline{\mathcal{P}} \cup \overline{\mathcal{Z}} \cup \mathcal{Z}_1)$  and  $S^a$  and  $S^{a\gamma}$  are constituent sequences of  $IS^a$ .

**Proof:** Here we make use of equations in Theorem 3.4.4. From (3.4.14)  $\sum \aleph(S^a) \aleph(S^{a\gamma}) = -2^{r-1} - \omega(2^r)$ , where summations is carried out through all  $m$ -sequences in  $\mathcal{P} \cup \mathcal{Z}$ . LHS of this equations can be split up into  $\sum_{a \in G_a / \{1, \gamma\}} \aleph(S^a) \aleph(S^{a\gamma}) + \sum_{a \in \gamma(G_a / \{1, \gamma\})} \aleph(S^a) \aleph(S^{a\gamma})$ , where  $S^a \in (\mathcal{P} \cup \mathcal{Z})$ . As in Lemma 3.5.2 both summands are equal, and LHS of (3.5.11) is accounted in  $\sum_{a \in G_a / \{1, \gamma\}} \aleph(S^a) \aleph(S^{a\gamma})$ , since  $m$ -sequences of subset  $\mathcal{P} \cup \mathcal{Z}$  are present only in the subset  $(\overline{\mathcal{P}} \cup \overline{\mathcal{Z}} \cup \mathcal{Z}_1)$  as constituent  $m$ -sequences. Then dividing 2 from (3.4.14) yields (3.5.11). Similarly (3.5.12) can be proved using (3.4.15).  $\square$

When  $r$  is odd,  $\aleph$  value and the product of  $\aleph$  values of constituent  $m$ -sequences, of Im-sequences in the subsets  $\overline{\mathcal{P}}, \overline{\mathcal{Z}}, \mathcal{Z}_1$  are as follows

Solving the above equations, for both the cases when  $r$  is odd and even, the cardinality of the subsets  $\overline{\mathcal{P}}, \overline{\mathcal{Z}}, \overline{\mathcal{R}}, \overline{\mathcal{S}}$  are computed and the results are tabulated in Table 3.5.1.

*Case 2 ( $\text{tr}(\tilde{\gamma}) = 0$ ):*

In this case, there are five modified subsets having common  $\aleph$  values; they are, with their constituent associations, given by  $\overline{\mathcal{P}} = (\mathcal{P} \& \mathcal{A}), \overline{\mathcal{Z}} = (\mathcal{Z} \& \mathcal{Z}), \overline{\mathcal{R}} = (\mathcal{R} \& \mathcal{R}), \overline{\mathcal{S}} = (\mathcal{S} \& \mathcal{S})$ , and a subset  $\mathcal{Z}_1 \cup \mathcal{Z}_2 \{ \mathcal{Z}_1 = (\mathcal{P} \& \mathcal{Z}) \mathcal{Z}_2 = (\mathcal{R} \& \mathcal{S}) \}$ , where  $\cup$  represents set theoretic union. Again, the volume constraint implies

$$|\overline{\mathcal{P}}| + |\overline{\mathcal{Z}}| + |\overline{\mathcal{R}}| + |\overline{\mathcal{S}}| + (|\mathcal{Z}_1| + |\mathcal{Z}_2|) = 2^{r-1}. \quad (3.5.9)$$

Also constituent sequences of Im-sequences in the subset  $\overline{\mathcal{P}} \cup \overline{\mathcal{Z}} \cup \mathcal{Z}_1$  accounts for all  $m$ -sequences from the subset  $\mathcal{P} \cup \mathcal{Z}$  whose size is  $2^{r-1}$ . This along with (3.5.9) then implies

$$|\overline{\mathcal{P}}| + |\overline{\mathcal{Z}}| + |\mathcal{Z}_1| = 2^{r-2} = |\overline{\mathcal{R}}| + |\overline{\mathcal{S}}| + (|\mathcal{Z}_2|) \quad (3.5.10)$$

Arguments for cardinality computations of subsets runs similar to the previous case, except here we have to make use of (3.4.14) and (3.4.15). Lemma 3.5.3 is useful for calculating cardinalities.

**Lemma 3.5.3:** For  $\gamma \neq 1, 3$  with  $\text{tr}(\tilde{\gamma}) = 0$ ,

$$\sum \aleph(S^a) \aleph(S^{a\gamma}) = -2^{r-2} - \omega(2^{r-1}); \quad r: \text{odd} \quad (3.5.11)$$

$$\sum \aleph(S^a) \aleph(S^{a\gamma}) = -3 \cdot 2^{r-2}; \quad r: \text{even} \quad (3.5.12)$$

where summation is carried over all Im-sequences  $IS^a$  in the subset  $(\overline{\mathcal{P}} \cup \overline{\mathcal{Z}} \cup \mathcal{Z}_1)$  and  $S^a$  and  $S^{a\gamma}$  are constituent sequences of  $IS^a$ .

**Proof:** Here we make use of equations in Theorem 3.4.4. From (3.4.14)  $\sum \aleph(S^a) \aleph(S^{a\gamma}) = -2^{r-1} - \omega(2^r)$ , where summations is carried out through all  $m$ -sequences in  $\mathcal{P} \cup \mathcal{Z}$ . LHS of this equations can be split up into  $\sum_{a \in G_a / \{1, \gamma\}} \aleph(S^a) \aleph(S^{a\gamma}) + \sum_{a \in \gamma(G_a / \{1, \gamma\})} \aleph(S^a) \aleph(S^{a\gamma})$ , where  $S^a \in (\mathcal{P} \cup \mathcal{Z})$ . As in Lemma 3.5.2 both summands are equal, and LHS of (3.5.11) is accounted in  $\sum_{a \in G_a / \{1, \gamma\}} \aleph(S^a) \aleph(S^{a\gamma})$ , since  $m$ -sequences of subset  $\mathcal{P} \cup \mathcal{Z}$  are present only in the subset  $(\overline{\mathcal{P}} \cup \overline{\mathcal{Z}} \cup \mathcal{Z}_1)$  as constituent  $m$ -sequences. Then dividing 2 from (3.4.14) yields (3.5.11). Similarly (3.5.12) can be proved using (3.4.15).  $\square$

When  $r$  is odd,  $\aleph$  value and the product of  $\aleph$  values of constituent  $m$ -sequences, of Im-sequences in the subsets  $\overline{\mathcal{P}}, \overline{\mathcal{Z}}, \mathcal{Z}_1$  are as follows

Subsets	Association	$\aleph(\text{IS}^a)$	$\aleph(\text{S}^a)\aleph(\text{S}^{a\gamma})$
$\mathcal{P}$	$(\mathcal{P} \& \mathcal{P})$	$2(2^t - 1 + \omega 2^t)$	$1 - 2^{t+1} + \omega 2(2^{2t} - 2^t)$
$\mathcal{Z}$	$(\mathcal{Z} \& \mathcal{Z})$	$2(-2^t - 1 - \omega 2^t)$	$1 + 2^{t+1} + \omega 2(2^{2t} + 2^t)$
$\mathcal{Z}_1$	$(\mathcal{P} \& \mathcal{Z})$	$-2$	$1 - \omega 2^t$

By the symmetry argument, volume constraint, (3.5.7) and Lemma 3.5.3, we have

$$\begin{aligned}
 |\mathcal{P}| &= |\mathcal{R}|, |\mathcal{Z}| = |\mathcal{O}| \text{ and } |\mathcal{Z}_1| = |\mathcal{Z}_2|, \\
 2^{t+1}(|\mathcal{P}| - |\mathcal{Z}|) &= 2(|\mathcal{P}| + |\mathcal{Z}| + |\mathcal{Z}_1|) = 2(|\mathcal{R}| + |\mathcal{O}| + |\mathcal{Z}_2|) = 2^{r-1}, \\
 |\mathcal{P}| + |\mathcal{Z}| &= |\mathcal{Z}_1|.
 \end{aligned}$$

Similarly when  $r$  is even, by the symmetry argument, from volume constraint, from (3.5.10), from (3.5.7) and from Lemma 3.5.3 we have

$$\begin{aligned}
 |\mathcal{R}| &= |\mathcal{O}|, |\mathcal{Z}_1| = |\mathcal{Z}_2|, \\
 2^t(|\mathcal{P}| - |\mathcal{Z}|) &= 2(|\mathcal{P}| + |\mathcal{Z}| + |\mathcal{Z}_1|) = 2(2|\mathcal{R}| + |\mathcal{Z}_2|) = 2^{r-1} \text{ and} \\
 |\mathcal{P}| + |\mathcal{Z}| &= |\mathcal{Z}_1|.
 \end{aligned}$$

Solution of above equations yields cardinalities of the subsets. The results are given in Table 3.5.2.

**Theorem 3.5.1:** The  $\aleph$  and Weight distributions of the families of Im-sequences over  $Z_4$  of period  $2(2^r - 1)$  are given in Tables 3.5.1, 3.5.2, 3.5.3. In all these tables, for all the items except the last,  $w_2 = (2^r - 2) - w_0$ ,  $w_3 = 2^r - w_1$ ; for the last item,  $w_3 = 0$ ,  $w_2 = 2^r$

*Example 3.5.1:* Families of im-sequences of period 30; three representative examples for different types of  $\mathcal{N}$  families are given in Table 3.5.4; Galois ring elements are represented as vectors over  $Z_4$ .

*Example 3.5.2:* Families of im-sequences of period 62; three representative examples for different types of  $\mathcal{N}$  families are given in Table 3.5.5; Galois ring elements are represented as vectors over  $Z_4$ .

Table 3.5.1 Correlation Transform and Weight Distributions of  $\mathcal{NM}(\text{tr}(\tilde{\gamma})=1)$ (a)  $r$  : Odd Integer,  $r = 2t+1$ ; Period =  $2(2^r-1)$ 

Sl. No.	SUB SET	$\aleph$	No of seques in the SUBSET	Constituent association	$w_0$	$w_1$
1.	$\overline{\mathcal{P}}$	$2(2^t-1)$	$2^{t-1}(2^{t-1}+1)$	$\eta \in \mathcal{P}, \eta\gamma \in \mathcal{R}$	$2^{2t}+2^t-2$	$2^{2t}$
2.	$\overline{\mathcal{Z}}$	$-2(2^t+1)$	$2^{t-1}(2^{t-1}-1)$	$\eta \in \mathcal{Z}, \eta\gamma \in \mathcal{S}$	$2^{2t}-2^t-2$	$2^{2t}$
3.	$\overline{\mathcal{R}}$	$-2 + \omega 2^{t+1}$	$2^{2t-2}$	$\eta \in \mathcal{P}, \eta\gamma \in \mathcal{S}$	$2^{2t}-2$	$2^{2t}+2^t$
4.	$\overline{\mathcal{S}}$	$-2 - \omega 2^{t+1}$	$2^{2t-2}$	$\eta \in \mathcal{Z}, \eta\gamma \in \mathcal{R}$	$2^{2t}-2$	$2^{2t}-2^t$
5		$-2$	1	$\eta \in < 2 >$	$2^r-2$	0

(b)  $r$  : Even Integer,  $r = 2t$ ; Period =  $2(2^r-1)$ 

Sl. No.	SUB SET	$\aleph$	No of seques in the SUBSET	Constituent association	$w_0$	$w_1$
1.	$\overline{\mathcal{P}}$	$(2^t-2 + \omega 2^t)$	$2^{t-2}(2^{t-1}+1)$	$\eta \in \mathcal{P}, \eta\gamma \in \mathcal{R}$	$2^{r-1}+2^{t-1}-2$	$2^{r-1}+2^{t-1}$
2.	$\overline{\mathcal{Z}}$	$(-2^t-2 - \omega 2^t)$	$2^{t-2}(2^{t-1}-1)$	$\eta \in \mathcal{Z}, \eta\gamma \in \mathcal{S}$	$2^{r-1}-2^{t-1}-2$	$2^{r-1}-2^{t-1}$
3.	$\overline{\mathcal{R}}$	$(2^t-2 - \omega 2^t)$	$2^{t-2}(2^{t-1}+1)$	$\eta \in \mathcal{P}, \eta\gamma \in \mathcal{S}$	$2^{r-1}+2^{t-1}-2$	$2^{r-1}-2^{t-1}$
4.	$\overline{\mathcal{S}}$	$(-2^t-2 + \omega 2^t)$	$2^{t-2}(2^{t-1}-1)$	$\eta \in \mathcal{Z}, \eta\gamma \in \mathcal{R}$	$2^{r-1}-2^{t-1}-2$	$2^{r-1}+2^{t-1}$
5.	$-2$	1	$\eta \in < 2 >$	$2^r-2$	0	

Table 3.5.2 Correlation Transform and Weight Distributions of  $\mathcal{NM}(\text{tr}(\gamma)=0)$ (a)  $r$  : Odd Integer,  $r = 2t+1$ ; Period =  $2(2^t-1)$ 

Sl. No.	SUB SET	$\mathfrak{K}$	No of seques in the SUBSET	Constituent association	$w_0$	$w_1$
1.	$\overline{\mathcal{P}}$	$2(2^t-1 + \omega 2^t)$	$2^{t-2}(2^{t-1}+1)$	$\eta \in \mathcal{P}, \eta\gamma \in \mathcal{P}$	$2^{2t}+2^t-2$	$2^{2t}+2^t$
2.	$\overline{\mathcal{Z}}$	$2(-2^t-1 - \omega 2^t)$	$2^{t-2}(2^{t-1}-1)$	$\eta \in \mathcal{Z}, \eta\gamma \in \mathcal{Z}$	$2^{2t}-2^t-2$	$2^{2t}-2^t$
3.	$\overline{\mathcal{R}}$	$2(2^t-1 - \omega 2^t)$	$2^{t-2}(2^{t-1}+1)$	$\eta \in \mathcal{R}, \eta\gamma \in \mathcal{R}$	$2^{2t}+2^t-2$	$2^{2t}-2^t$
4.	$\overline{\mathcal{O}}$	$2(-2^t-1 + \omega 2^t)$	$2^{t-2}(2^{t-1}-1)$	$\eta \in \mathcal{O}, \eta\gamma \in \mathcal{O}$	$2^{2t}-2^t-2$	$2^{2t}+2^t$
5.		-2	$2^{2t-1}$	$\eta \in \mathcal{P}, \eta\gamma \in \mathcal{Z}$ $\eta \in \mathcal{R}, \eta\gamma \in \mathcal{O}$	$2^{2t}-2$	$2^{2t}$
6.		-2	1	$\eta \in \langle 2 \rangle$	$2^t-2$	0

(b)  $r$  : Even Integer,  $r = 2t$ ; Period =  $2(2^t-1)$ 

Sl. No.	SUB SET	$\mathfrak{K}$	No of seques in the SUBSET	Constituent association	$w_0$	$w_1$
1.	$\overline{\mathcal{P}}$	$2(2^t-1)$	$2^{t-2}(2^{t-2}+1)$	$\eta \in \mathcal{P}, \eta\gamma \in \mathcal{P}$	$2^{r-1}+2^t-2$	$2^{r-1}$
2.	$\overline{\mathcal{Z}}$	$-2(2^t+1)$	$2^{t-2}(2^{t-2}-1)$	$\eta \in \mathcal{Z}, \eta\gamma \in \mathcal{Z}$	$2^{r-1}-2^t-2$	$2^{r-1}$
3.	$\overline{\mathcal{R}}$	$-2 + \omega 2^{t+1}$	$2^{2t-4}$	$\eta \in \mathcal{R}, \eta\gamma \in \mathcal{R}$	$2^{r-1}-2$	$2^{r-1}+2^t$
4.	$\overline{\mathcal{O}}$	$-2 - \omega 2^{t+1}$	$2^{2t-4}$	$\eta \in \mathcal{O}, \eta\gamma \in \mathcal{O}$	$2^{r-1}-2$	$2^{r-1}-2^t$
5.		-2	$2^{2t-2}$	$\eta \in \mathcal{P}, \eta\gamma \in \mathcal{Z}$ $\eta \in \mathcal{R}, \eta\gamma \in \mathcal{O}$	$2^{r-1}-2$	$2^{r-1}$
6.		-2	1	$\eta \in \langle 2 \rangle$	$2^t-2$	0



Table 3.5.3 Correlation Transform and Weight Distributions of  $\mathcal{N}^\gamma(\gamma = 3)$ (a)  $r$  : Odd Integer,  $r = 2t+1$ ; Period =  $2(2^r-1)$ 

Sl. No.	SUB SET	$\aleph$	No of seques in the SUBSET	Constituent association	$w_0$	$w_1$
1.	$\overline{\mathcal{P}}$	$2(2^t-1)$	$2^{t-1}(2^t+1)$	$\eta \in \mathcal{P}, \eta\gamma \in \mathcal{R}$	$2^{2t}+2^t-2$	$2^{2t}$
2.	$\overline{\mathcal{Z}}$	$-2(2^t+1)$	$2^{t-1}(2^t-1)$	$\eta \in \mathcal{Z}, \eta\gamma \in \mathcal{S}$	$2^{2t}-2^t-2$	$2^{2t}$
3	-2	1	$\eta \in < 2 >$	$2^r-2$	0	

(b)  $r$  : Even Integer,  $r = 2t$ ; Period =  $2(2^r-1)$ 

Family : $\mathcal{N}^\gamma(\gamma = 3)$		Period = $2(2^r-1)$			$r$ : even integer, $r = 2t$	
Sl. No.	SUB SET	$\aleph$	No of seques in the SUBSET	Constituent association	$w_0$	$w_1$
1.	$\overline{\mathcal{P}}$	$2(2^t-1)$	$2^{t-2}(2^{t-1}+1)$	$\eta \in \mathcal{P}, \eta\gamma \in \mathcal{P}$	$2^{r-1}+2^t-2$	$2^{r-1}$
2.	$\overline{\mathcal{Z}}$	$-2(2^t+1)$	$2^{t-2}(2^{t-1}-1)$	$\eta \in \mathcal{Z}, \eta\gamma \in \mathcal{Z}$	$2^{r-1}-2^t-2$	$2^{r-1}$
3	$\overline{\mathcal{R}}$	-2	$2^{2t-2}$	$\eta \in \mathcal{P}, \eta\gamma \in \mathcal{Z}$	$2^{r-1}-2$	$2^{r-1}$
4.		-2	1	$\eta \in < 2 >$	$2^r-2$	0

Table 3.5.4  $\mathcal{KM}$  Families of Period 30 (Example 3.5.1)a. Sequences of Family  $\mathcal{KM}^{\gamma}(\text{tr}(\bar{\gamma}) = 1; \gamma = (1002)$ 

$$\omega = \sqrt{-1}$$

Sequences are generated by  $\gamma\alpha$ ,  $\gamma = (1002)$ ,  $\alpha = (0100)$ ,  $\gamma\alpha = (2300)$

Minimal polynomial corresponding to  $\gamma\alpha$  is  $3+d+2d^2+d^4$

SL No	a	IS <sup>a</sup>	$\aleph(\text{IS}^a)$
1	(1000)	001023101233112003221123013110	$2+\omega 4$
2	(3000)	003021303211332001223321031330	$2-\omega 4$
3	(1200)	021001121011312023203103231310	$2+\omega 4$
4	(3200)	023003323033132021201301213130	$2-\omega 4$
5	(1020)	201203303011112203001321231110	$2+\omega 4$
6	(3020)	203201101033332201003123213330	$2-\omega 4$
7	(1220)	221221323233312223023301013310	$-6-\omega 4$
8	(3220)	223223121211132221021103031130	$-6+\omega 4$
9	(1000)	002002202022220002002202022220	$-2$

b. Sequences of Family  $\mathcal{KM}^{\gamma}(\text{tr}(\bar{\gamma}) = 0; \gamma = (1200)$ 

Sequences are generated by  $\gamma\alpha$ ,  $\gamma = (1200)$ ,  $\alpha = (0100)$ ,  $\gamma\alpha = (0120)$

Minimal polynomial corresponding to  $\gamma\alpha$  is  $1+3d+d^4$

SL No	a	IS <sup>a</sup>	$\aleph(\text{IS}^a)$
1	(1000)	003003103233310023021123011110	6
2	(3000)	001001301211130021023321033330	6
3	(1020)	203223301011310223201321233110	$-2$
4	(3020)	201221103033130221203123211330	$-2$
5	(1002)	001201121013312021223101231112	$-2+\omega 8$
6	(3002)	003203323031132023221303213332	$-2-\omega 8$
7	(1022)	201021323231312221003303013112	$-2$
8	(3022)	203023121213132223001101031332	$-2$
9	(1000)	002002202022220002002202022220	$-2$

Table 3.5.4: Continued..

c. Sequences of Family  $\mathcal{K}(\gamma = 3)$ Sequences are generated by  $\gamma\alpha$ ,  $\gamma = (3000)$ ,  $\alpha = (0100)$ ,  $\gamma\alpha = (0300)$ Minimal polynomial corresponding to  $\gamma\alpha$  is  $1+d+2d^2+d^4$ 

SL No	a	IS <sup>a</sup>	$\kappa(\text{IS}^a)$
1	(1000)	001023301233310003021103211130	6
2	(1200)	021001321011110023003123033330	6
3	(1020)	201203103011310203201301033130	6
4	(1220)	221221123233110223223321211330	-10
5	(1002)	003221323013312001223121031132	-2
6	(1202)	023203303231112021201101213332	-2
7	(1022)	203001121231312201003323213132	-2
8	(1222)	223023101013112221021303031332	-2
9	(1000)	0020022020222000200220202220	-2

Table 3.5.5  $\mathcal{K}$ families of period 62 (Example 3.5.2)a. Sequences of family  $\mathcal{K}(\text{tr}(\tilde{\gamma}) = 1; \gamma = (32000))$ Sequences are generated by  $\gamma\alpha$ ,  $\gamma = (32000)$ ,  $\alpha = (01000)$ ,  $\gamma\alpha = (03200)$ Minimal polynomial corresponding to  $\gamma\alpha$  is  $1+d^2+2d^3+d^5$ .

$$\omega = \sqrt{-1}$$

a	IS <sup>a</sup>	$\kappa(\text{IS}^a)$
(10000)	0010132011331220310133030322230232112211333222332131212122201	-10
(12000)	0212332233111222112313232322030030312033113220130311010122221	-10
(10200)	20321302331312023323310103220232210110033133200310333232122001	-2- $\omega 8$
(12200)	22303300113112001301112123220032012310211313202112113030122021	-2+ $\omega 8$
(10020)	0230110233331000132113230320221001213003333002110111012120203	6
(12020)	00323100111110023303330323202010210330211113000312331210120223	6
(10220)	22121120111310221103112103200212030132211133020132313032120003	-2+ $\omega 8$
(12220)	20103122333110203121310123200012232332033313022330133230120023	-2- $\omega 8$
(10002)	22103102313330221303310303022032032330031331020112333212102221	-2- $\omega 8$
(12002)	20121100131130203321112323022232230130213111022310113010102201	-2+ $\omega 8$
(10202)	02323120131330001121330103020030010332213131002130131232102021	6
(12202)	00301122313130023103132123020230212132031311000332311030102001	6
(10022)	20303320133332023123112303002012212312213331200330313012100223	-2- $\omega 8$
(12022)	22321322311132001101310323002212010112031111202132133210100203	-2+ $\omega 8$
(10222)	00123302311332203301132103000010230310031131222312111032100023	6
(12222)	02101300133132221323330123000210032110213311220110331230100003	6
(10000)	0020220022220002202220202000020022002222000220222020200002	-2

Table 3.5.5: Continued..

b. Sequences of Family  $\mathcal{K}^{\gamma}(\text{tr}(\bar{\gamma}) = 0; \gamma = (12000)$ Sequences are generated by  $\gamma\alpha$ ,  $\gamma = (12000)$ ,  $\alpha = (01000)$ ,  $\gamma\alpha = (01200)$ Minimal polynomial corresponding to  $\gamma\alpha$  is  $3+3d^2+2d^3+d^5$ 

a	IS <sup>a</sup>	K(IS <sup>a</sup> )
(10000)	0030332031133220110113030322210232132213313222312333232322201	-10- $\omega$ 8
(30000)	00101120133112203303310101222230212312231131222132111212122203	-10+ $\omega$ 8
(10200)	20123302133332021323110103220212210130031113200330131212322001	-2
(30200)	20321102311112023121330301220232230310013331200110313232122003	-2
(10020)	02103102131330003321332303202230012110031313002130313032320203	6- $\omega$ 8
(30020)	02301302313110001123112101202210032330013131002310131012120201	6+ $\omega$ 8
(10220)	22323120313330223103312103200232030112213113020112111012320003	-2
(30220)	22121320131110221301132301200212010332231331020332333032120001	-2)
(10002)	22301102111310223303110303022012032310033311020132131232302221	-2
(30002)	22103302333130221101330101022032012130011133020312313212102223	-2
(10202)	02121120333310003121130103020010010312211111002110333212302021	6+ $\omega$ 8
(30202)	02323320111130001323310301020030030132233333002330111232102023	6- $\omega$ 8)
(10022)	20101320331312021123312303002032212332211311200310111032300223	-2
(30022)	20303120113132023321132101002012232112233133200130333012100221	-2
(10222)	00321302113312201301332103000030230330033111222332313012300023	6- $\omega$ 8
(30222)	00123102331132203103112301000010210110011333222112131032100021	6+ $\omega$ 8
(10000)	002022002222000220222020200002002022002222000220222020200002	-2

c. Sequences of Family  $\mathcal{K}^{\gamma}(\gamma = 3)$ Sequences are generated by  $\gamma\alpha$ ,  $\gamma = (30000)$ ,  $\alpha = (01000)$ ,  $\gamma\alpha = (03000)$ Minimal polynomial corresponding to  $\gamma\alpha$  is  $1+2d+d^2+d^5$ 

a	IS <sup>a</sup>	K(IS <sup>a</sup> )
(10000)	0010332031131220112113232322230030112013313220332331212122221	-10
(12000)	0212132213311222310333030322030232312231133222130111010122201	-10
(10200)	20323302133312021303112123220232012110231113202310133232122021	-10
(12200)	22301300311112003321310103220032210310013333200112313030122001	6
(10020)	02303102131310003301330323202210210130231313000110311012120223	6
(12020)	00321100313110021323132303202010012330013133002312131210120203	6
(10220)	22123120313310223123310123200212232132013113022132113032120023	-10
(12220)	20101122131110201101112103200012030332231333020330333230120003	6
(10002)	22101102111330223323112323022032230330233311022112133212102201	-10
(12002)	20123100333130201301310303022232032130011131020310313010102221	6
(10202)	02321120333330003101132123020030212332011111000130331232102001	6
(12202)	00303122111130021123330103020230010132233331002332111030102021	6
(10022)	20301320331332021103310323002012010312011311202330113012100203	6
(12022)	22323322113132003121112303002212212112233131200132333210100223	-10
(10222)	00121302113332201321330123000010032310233111220312311032100003	6
(12222)	02103300331132223303132103000210230110011331222110131230100023	6
(10000)	002022002222000220222020200002002022002222000220222020200002	-2

### 3.5.3 Correlation Distribution

The linear property of the families allows us to relate the correlation distribution with the  $\aleph$  distribution as in the case of  $\mathcal{K}$  family. Number of sequences in a  $\mathcal{JK}$  family is  $2^{r-1}+1$ , and the period of all sequences except  $IS^2$  is  $2(2^r-1)$ , period of  $IS^2$  being  $2^r-1$ . The correlation values belong to the set:

$$\{ \aleph (IS^a - T^1(B)), \text{ for all } IS^a \in \mathcal{JK}^\gamma, \tau \in Z_{2(2^r-1)}, B \in (\mathcal{JK}^\gamma) \} \quad (3.5.13)$$

where  $T^1(\cdot)$  represents 1<sup>th</sup> shift  $(\cdot)$ . Since  $\mathcal{JK}$  family is linear, the set (3.5.13) is expressed as

$$\begin{aligned} & \{ \aleph(IS^0) \}^{2^{r-1}+1} \cup ( \{ \aleph(IS^b, b = IS^2) \}^{(2^{r-1}+1)(2^r-1)} \setminus \{ \aleph(IS^a), a = IS^2 \} ) \\ & \cup ( \{ \aleph(IS^b, b \in \mathcal{JK}) \}^{2(2^r-1)(2^{r-1}+1)} \setminus \{ \aleph(IS^a), IS^a \in \mathcal{JK} \} ), \end{aligned}$$

where  $\cup$  represents set theoretic union. The second term in the above expression, has multiplicity factor of  $(2^{r-1}+1)(2^r-1) - 1$ , since the period of  $IS^2$  is only  $2^r-1$ . Thus correlation distributions are obtained by modifying the  $\aleph$  distributions as follows:

- (1) Include a correlation entry of  $2(2^r-1)$  occurring  $2^{r-1}+1$  times.
- (2) For every  $\aleph$  entry except that corresponding to  $IS^2$ , number of occurrences is obtained by multiplying  $(2^{2r}+2^r-3)$  to a value in 'No of Occurrences' column of that entry.
- (3) For the entry corresponding to  $IS^2$  ( $\aleph$  value is  $-2$ ), no of occurrences is given by  $(2^{2r}+2^{r-1}-2)$ .

Table 3.5.6 summarizes various properties of quadriphase families derived in this chapter.

## 3.6 Maximal Length Sequences over $Z_8$

This section discusses construction of octaphase sequences derived from maximal length sequences over  $Z_8$ . There are three level maximal length sequences over  $Z_8$ , first and second level sequences are isomorphic to  $Z_4$  and  $Z_2$  m-sequences respectively. Only zeroth level sequences are considered here.

### 3.6.1 Construction of octaphase sequences

Octaphase sequences are constructed from sequences over  $Z_8$  through octaphase mapping  $\phi$  from  $Z_8$  to eight roots of unity is given by

$$\phi(x) = \exp(\omega \frac{2\pi x}{8}), x \in Z_8, \omega = \sqrt{-1}. \quad (3.6.1)$$

If  $A = \{a_i\}$ , a sequence over  $Z_8$  of period  $L$ , then octaphase sequence  $X$  derived from  $A$  is given by

$$X = \{x_i; i=0..L-1\}; x_i = (\omega)^{a_i}, \exp(\omega \frac{2\pi}{8})^{a_i}.$$

Correlation transform of a sequence A of period L over  $Z_8$ , for this case, is given by

$$\aleph(A) = \sum_{i=0}^{L-1} \exp(\omega \frac{2\pi}{8})^{a_i}. \quad (3.6.2)$$

Let  $W^A$  be the weight vector associated with a sequence A, which is a integer valued vector of length 8 such that  $w_i^A$  is the number of symbols i present in A. The correlation transform of A, then becomes (refer (2.1.10))

$$\aleph(A) = \left\{ (w_0^A - w_4^A) + \omega (w_2^A - w_6^A) \right\} + \frac{1}{\sqrt{2}} \left\{ [(w_1^A + w_7^A) - (w_3^A + w_5^A)] + \omega [(w_1^A - w_7^A) + (w_3^A - w_5^A)] \right\}.$$

Since  $Z_8$  is a matched alphabet for octaphase correlation, the periodic crosscorrelation between X and Y becomes  $C_{XY}(\tau) = \aleph(A-B)$ , where A-B is pointwise sequence subtraction modulo 8. Hence the

Table 3.5.6 Properties of Quadriphase Families

Family	Period	Family size	Linear span	$(C_{\max})^2$	Comment
$\mathcal{K}$	$2^r-1$ (r : odd)	$2^r+1$	r	$1+ 2^r \pm 2^{(r+1/2)}$	Optimal (Welch)
$\mathcal{K}$	$2^r-1$ (r : even)	$2^r+1$	r	$1+ 2^r$ or $1+ 2^r \pm 2^{(r+2/2)}$	Optimal (Welch)
$\mathcal{JK}'$ $\text{tr}(\gamma)=1$	$2(2^r-1)$ (r : odd)	$2^{r-1}+1$	r	$2(2+ 2^r)$ or $2(2+ 2^r \pm 2^{(r+1/2)})$	Optimal (Welch)
$\mathcal{JK}'$ ( $\gamma=3$ )	$2(2^r-1)$ (r : odd)	$2^{r-1}+1$	r	$2(2+ 2^r \pm 2^{(r+1/2)})$	Optimal (Welch)
$\mathcal{JK}'$ $\text{tr}(\tilde{\gamma})=0$	$2(2^r-1)$ (r : odd)	$2^{r-1}+1$	r	$4(1+ 2^r \pm 2^{(r+1/2)})$	Sub optimal
$\mathcal{JK}'$ $\text{tr}(\tilde{\gamma})=1$	$2(2^r-1)$ (r : even)	$2^{r-1}+1$	r	$2(2+ 2^r \pm 2^{(r+2/2)})$	Optimal (Welch)
$\mathcal{JK}'$ ( $\gamma=3$ )	$2(2^r-1)$ (r : even)	$2^{r-1}+1$	r	$4(1+ 2^r \pm 2^{(r+2/2)})$	Sub optimal
$\mathcal{JK}'$ $\text{tr}(\tilde{\gamma})=0$	$2(2^r-1)$ (r : even)	$2^{r-1}+1$	r	$4(1+ 2^r \pm 2^{(r+1/2)})$ or $4(1+ 2^r)$	Sub optimal

computation of crosscorrelation of any two quadriphase sequences reduces to calculating the weight vector associated with the difference of their corresponding  $Z_4$  sequences. At the outset it might appear that the method of correlation computation through association schemes can be applied here also as in the case of  $m$ -sequences over  $Z_4$ . The appropriate ring on which association scheme can be defined in this case is  $GR(8,r)$ . Number of classes in the association scheme is  $4^r + 2^r + 1$ . But the computations of intermediate numbers of the scheme are extremely tedious. Thus we will not attempt to find exact nature of  $K$ 's. Instead we identify subsets of zeroth level sequences which satisfy Welch bound with equality (Section 2.5.1). This implies that  $\theta_{rms}$  for the subsets of sequences is approximately equal to  $\sqrt{L}$ ,  $L$ :period. But out-of-phase correlations occasionally exceed  $\sqrt{L}$ , which is the optimal value according Welch's bound on  $\theta_{max}$ .

### 3.6.2 Sequence Sets Satisfying Welch's Bound With Equality

Associated with every element  $a$  of  $GR^*(8,r)$ , an  $m$ -sequence  $S^a = \{s_i\}$  is given by

$$s_i = \text{tr}_1^r(a\alpha^i), i \in Z_{2^r-1}.$$

The distinct zeroth level sequences are given by the set  $\{S^a, a \in G_a\}$ , which accounts for  $4^r$  sequences, where  $G_a$  is the Abelian component group of  $GR^*(8,r)$ . As in the case of  $Z_4$   $m$ -sequences, number of distinct families is given by  $\phi(2^r-1)/r$ , where  $\phi$  is the Euler's  $\phi$  function.

We consider  $2^r$  sets of  $2^r$   $m$ -sequences satisfying Welch's bound with equality. The  $4^r$  zeroth level  $m$ -sequences are divided into  $2^r$  sets. To index different distinct zeroth level sequences the additive representation of  $G_a$  is used. Any element of  $G_a$  of  $GR^*(8,r)$  can be represented as  $a = 1 + 2a'$ , where  $a' \in GR(4,r)$ . From P7 and P8 of Section 3.1,  $a'$  can in turn be expressed as  $a' = 2^i(1 + 2e')\alpha$ , where  $\alpha, e' \in G_c$  of  $GR^*(4,r)$  and  $i=0$  or  $1$ . Then, since cyclic component groups,  $G_c$ 's, of  $GR^*(4,r)$  and  $GR^*(8,r)$  are isomorphic, any  $a \in GR^*(8,r)$  can be expressed as

$$a = (1 + 2\tilde{a} + 4\hat{a}), \quad (3.6.3)$$

where  $\tilde{a}$  and  $\hat{a}$  belongs to  $\{G_c \cup 0\}$ , where  $\cup$  represents set theoretic union.  $2^r$  sets of octaphase sequences are described as given below. For unique  $\tilde{a} \in \{G_c \cup 0\}$ , a set of sequences,  $\mathcal{K}(\tilde{a})$  is defined. The members of  $\mathcal{K}(\tilde{a})$  are given by the set

$$\{S^a, a = 1 + 2\tilde{a} + 4\hat{a}, \text{ for all } \hat{a} \in \{G_c \cup 0\}\}. \quad (3.6.4)$$

### 3.6.3 Number of Distinct Octo-phase Sequence Sets

For each distinct family of  $\mathcal{K}$ , we have  $2^r$  sequence sets. There are  $\phi(2^r-1)/r$  different  $\mathcal{K}$  families. Thus total number of sequence sets are given by

$$2^r(\phi(2^r-1)/r),$$

where  $\phi$  is Euler's  $\phi$  function.

### 3.6.4 Correlation computations of m-sequences over $Z_8$

In this subsection we show that sets  $\mathcal{K}(\tilde{a})$  defined above satisfy Welch bound with equality. This implies that  $\theta_{\text{rms}}$  for the sequence sets is approximately equal to  $\sqrt{L}$ ,  $L$  is the period of the sequences. They are useful in CDMA communication systems which employ 8-PSK modulation.

**Lemma 3.6.1:** For any  $\alpha \in G_c$  and  $\tilde{a} \in GF(2^r)$ , the set of vectors,  $F^\alpha$

$$\{S^{\alpha a}, \text{ for } a = 1 + 2\tilde{a} + 4\hat{a}, \tilde{a} \text{ takes all values of } \{G_c \cup 0\}\}$$

satisfies Welch bound with equality.

**Proof:** Let us compute total energy (TE) of  $F^\alpha$  which is sum of all mutual inner-products between vectors; it is given by

$$TE = \sum_{n=1}^M \sum_{m=1}^M |C_{mn}(0)|^2 = \sum_{n=1}^M |C_{nn}(0)|^2 + \sum_{n=1}^M \sum_{m=1, m \neq n}^M |C_{mn}(0)|^2, \text{ where } M = 2^r. \quad (3.6.5)$$

Consider any two vectors  $S^{\alpha a}$  and  $S^{\alpha b}$ ,  $a = (1+2\tilde{a}+4\hat{a})$  and  $b = (1+2\tilde{b}+4\hat{b})$  belonging  $F^\alpha$ . The inner-product between  $S^{\alpha a}$  and  $S^{\alpha b}$  is then given by

$$C_{ab}(0) = \Re(S^{\alpha a} S^{\alpha b}) = \Re(S^{\alpha(a-b)}) = \Re(S^{\alpha(4(\hat{a}-\hat{b}))}).$$

If  $a = b$ , then  $\hat{a}-\hat{b}$  is zero and consequently  $C_{aa}(0) = 2^r-1$ , since  $\Re(S^0) = 2^r-1$ . If  $a \neq b$ , then  $S^{\alpha(4(\hat{a}-\hat{b}))}$  is an m-sequence over ideal  $\langle 4 \rangle$  which is isomorphic to  $GF(2)$  and consequently has  $\Re$  value as  $-1$ . Thus the inner-product  $C_{ab}(0)$ ,  $a \neq b$  is  $-1$ . Applying these results in (3.6.5), TE becomes

$$TE = 2^r (2^r-1)^2 + 2^r(2^r-1) (-1)^2 = 4^r(2^r-1) = \frac{(M \ E)^2}{L}$$

where  $M = 2^r$ ,  $E$  = energy of the signals  $= 2^r-1$ ,  $L$ : period  $= 2^r-1$ . Then from the Appendix E, the set of vectors satisfy Welch's bound with equality.  $\square$



**Theorem 3.6.1:** Sets of octaphase sequences derived from  $\mathcal{K}(\bar{a})$ ,  $\bar{a} \in \text{GR}(2, r)$ , satisfy Welch's bound with equality and hence mean square of the crosscorrelations,  $C_{\text{rms}}^2$  is approximately equal to the period of sequences,  $2^r - 1$ .

**Proof:** From Lemma 3.6.1, for any  $\alpha$ , the set  $F^\alpha$  satisfies Welch bound with equality. Then Theorem 2.5.2 implies that  $\bigcup_{\alpha \in G_c} (F^\alpha)$  also satisfies Welch bound with equality, where  $\bigcup$  represents set theoretic union. The vectors in the set  $\bigcup_{\alpha \in G_c} (F^\alpha)$ , accounts for all shifts of sequences in  $\mathcal{K}(\hat{a})$ . Then from Theorem 2.5.3 result follows.  $\square$

**Example 3.6.1:** List of all Sets  $\mathcal{K}(\bar{a})$ ,  $\bar{a} \in \{G_c \cup 0\}$  derived from from m-sequences over  $Z_8$  of period 7 generated by  $\alpha \in G_c$  of  $\text{GR}(8, 3)$  such that  $1 + 3\alpha + 2\alpha^2 = \alpha^3$ . Sequence sets are given in Table 3.6.1. The minimum polynomial  $m_\alpha(d) = 7 + 5d + 6d^2 + d^3$ .

Table 3.6.1 Sequences of  $\mathcal{K}(\bar{a})$ , for All  $\bar{a} \in \{G_c \cup 0\}$

Galois ring elements are represented as vectors over  $Z_8$

$$\omega = \sqrt{-1}$$

a. Family  $\mathcal{K}(\bar{a})$ ;  $\bar{a} = (010)$

(a)	Sequence $S^a$	$\Re(S^a)$
(120)	6 4 1 4 7 3 7	$-0.6 + \omega - 1.0$
(160)	6 0 1 0 3 7 7	$3.4 + \omega - 1.0$
(124)	2 4 5 0 3 3 7	$-1.4 + \omega 1.0$
(164)	2 0 5 4 7 7 7	$1.4 + \omega - 1.8$
(560)	6 0 5 0 7 3 3	$0.6 + \omega - 1.0$
(520)	6 4 5 4 3 7 3	$-3.4 + \omega - 1.0$
(564)	2 0 1 4 3 3 3	$-1.4 + \omega 3.8$
(524)	2 4 1 0 7 7 3	$1.4 + \omega 1.0$

Table 3.6.1 : Continued..

e. Family  $\mathcal{K}(\bar{a})$ ;  $\bar{a} = (775)$ 

(a)	Sequence $S^a$	$\mathcal{K}(S^a)$
(762)	4 0 1 6 7 1 5	$1.4 + \omega - 1.0$
(326)	0 4 1 6 3 1 1	$1.4 + \omega 1.8$
(366)	0 0 1 2 7 5 1	$3.4 + \omega 1.0$
(722)	4 4 1 2 3 5 5	$-3.4 + \omega 1.0$
(362)	4 0 5 6 3 5 1	$-1.4 + \omega - 1.0$
(726)	0 4 5 6 7 5 5	$-1.4 + \omega - 3.8$
(766)	0 0 5 2 3 1 5	$0.6 + \omega 1.0$
(322)	4 4 5 2 7 1 1	$-0.6 + \omega 1.0$

f. Family  $\mathcal{K}(\bar{a})$ ;  $\bar{a} = (561)$ 

(a)	Sequence $S^a$	$\mathcal{K}(S^a)$
(342)	0 6 1 4 1 7 5	$1.4 + \omega - 1.0$
(746)	4 6 1 0 1 3 1	$1.4 + \omega 1.8$
(742)	0 6 5 4 5 3 1	$-1.4 + \omega - 1.0$
(346)	4 6 5 0 5 7 5	$-1.4 + \omega - 3.8$
(302)	0 2 1 0 5 3 5	$0.6 + \omega 1.0$
(706)	4 2 1 4 5 7 1	$-0.6 + \omega 1.0$
(702)	0 2 5 0 1 7 1	$3.4 + \omega 1.0$
(306)	4 2 5 4 1 3 5	$-3.4 + \omega 1.0$

g. Family  $\mathcal{K}(\bar{a})$ ;  $\bar{a} = (100)$ 

(a)	Sequence $S^a$	$\mathcal{K}(S^a)$
(300)	6 6 7 6 7 7 1	$2.8 + \omega - 4.4$
(700)	6 6 3 6 3 3 5	
(340)	6 2 7 2 3 3 1	$0.0 + \omega 2.4$
(740)	6 2 3 2 7 7 5	$0.0 + \omega - 0.4$
(304)	2 6 3 2 3 7 1	$0.0 + \omega 2.4$
(704)	2 6 7 2 7 3 5	$0.0 + \omega - 0.4$
(344)	2 2 3 6 7 3 1	$0.0 + \omega 2.4$
(744)	2 2 7 6 3 7 5	$0.0 + \omega - 0.4$

h. Family  $\mathcal{K}(\bar{a})$ ;  $\bar{a} = (000)$ 

(a)	Sequence $S^a$	$\mathcal{K}(S^a)$
(100)	2 2 5 2 5 5 3	$-2.8 + \omega 1.6$
(500)	2 2 1 2 1 1 7	$2.8 + \omega 4.4$
(140)	2 6 5 6 1 1 3	$0.0 + \omega 0.4$
(540)	2 6 1 6 5 5 7	$0.0 + \omega - 2.4$
(104)	6 2 1 6 1 5 3	$0.0 + \omega 0.4$
(504)	6 2 5 6 5 1 7	$0.0 + \omega - 2.4$
(144)	6 6 1 2 5 1 3	$0.0 + \omega 0.4$
(544)	6 6 5 2 1 5 7	$0.0 + \omega - 2.4$

## Chapter 4

### Maximal Length Sequences over Local Residue Class Polynomial Rings

This chapter discusses generation and properties of maximal length sequences over residue class polynomial rings and their applications in constructing frequency hopping patterns and sequences with good block inner-product autocorrelations. Since, in general, any semi-local ring can be expressed as a direct sum of its local constituents, only local rings are considered here. A local residue class polynomial ring  $P_p^n[w^k(\xi)]$ , where  $w(\xi)$  is an irreducible polynomial over  $GF(p)$ ,  $\deg(w(\xi))=m$ ,  $k>1$ ,  $n=mk$ , will, in short, be denoted by  $P_p^n[w^k]$  by dropping the indeterminate  $\xi$  in the polynomial symbol  $w(\xi)$  whenever the context is clear. Relevant algebraic properties of  $P_p^n[w^k]$  are given in Appendix D. Definition and generation mechanism of trace sequence families are similar to those described for  $Z_{2^k}$ . Here the Galois extension ring of  $P_p^n[w^k]$ ,  $PGR(V^k, r)$ , plays a vital role.

The chapter is organized as follows. Section 4.1 gives vector space structure of  $P_p^n[w^k]$  and  $PGR(V^k, r)$  and their relevant properties. Section 4.2 defines families of trace sequences over  $P_p^n[w^k]$ . Definition and properties of maximal length sequences over  $P_p^n[w^k]$  are discussed in Section 4.3 and 4.4. Families of frequency hopping patterns derived from  $m$ -sequences are given in Section 4.5. Constructions of sequences with ideal block inner-product correlations are given Section 4.6.

#### 4.1 Vector Space Structure of $P_p^n[w^k]$ and $PGR(V^k, r)$

Relevant properties of  $P_p^n[w^k]$  and  $PGR(V^k, r)$ , as required for this thesis, are given in Appendix D. Main feature of  $P_p^n[w^k]$  and  $PGR(V^k, r)$  is their vector space structure.  $P_p^n[w^k]$  is a vector space of dimension  $n$  over  $GF(p)$  and  $PGR(V^k, r)$  is a vector space of dimension  $k$  over the subfield  $SPGR(V, r) = GF(V^r)$ . Three different types of representations are considered.

##### 4.1.1 Representations of $P_p^n[w^k]$

Since  $P_p^n[w^k]$  is a vector space of dimension  $n$  over  $GF(p)$ , the elements of  $P_p^n[w^k]$  can be expressed as vectors over  $GF(p)$  (as arrays of degree  $\leq n$  over  $GF(p)$ ). Let  $\xi^i$ ,  $i \in 0, \dots, n-1$ , be a vector with entry of 1 in  $i^{\text{th}}$  position and zero elsewhere. The vectors  $1, \xi, \xi^2, \dots, \xi^{n-1}$  form a basis, called standard basis. Any

element  $a$  of  $P_p^n[w^k]$  is expressed as

$$a = a_0 + a_1\xi + \dots + a_{r-1}\xi^{n-1}, \quad (4.1.1)$$

where  $a_i$ 's belong to  $GF(p)$ . This representation is referred to as **standard basis representation** of  $P_p^n[w^k]$ . The other two representations of  $P_p^n[w^k]$  are with respect to the set of vectors  $\{1, w(\xi), w^2(\xi), \dots, w^{k-1}(\xi)\}$ . It is easy to verify that the elements in the set  $\{1, w(\xi), w^2(\xi), \dots, w^{k-1}(\xi)\}$  are linearly independent over residue field of  $P_p^n[w^k]$  or subfield of  $P_p^n[w^k]$  and hence constitute a basis, called **ideal basis** since these basis vectors, as polynomials in  $\xi$ , generate all the ideals of the ring  $P_p^n[w^k]$ . The two representations using the ideal basis are:

(1) **Ideal basis representation I:** Here the elements of  $P_p^n[w^k]$  are expressed as linear sums of elements of residue field  $P_p^m[w]$ . The residue field  $P_p^m[w]$  is obtained by the natural homomorphic mapping (by taking modulo  $w(\xi)$ ) on the elements of  $P_p^n[w^k]$ . Any element  $b(\xi)$  can be expressed as

$$b(\xi) = B_0 + B_1w^1 + \dots + B_{k-1}w^{k-1}, \quad (4.1.2)$$

where  $B_i$ 's  $\in P_p^m[w]$  and are obtained from  $b(\xi)$  recursively by Euclid's algorithm:

$$B_0 = b(\xi) \bmod w(\xi), \quad Q_0 = b(\xi) \operatorname{div} w(\xi)$$

$$\text{and } B_j = Q_{j-1} \bmod w(\xi), \quad Q_j = Q_{j-1} \operatorname{div} w(\xi) \text{ for } j \geq 1.$$

(2) **Ideal Representation II :** Here the elements of  $P_p^n[w^k]$  are expressed as linear sums of subfields  $SP_p^m[w]$ . Any element  $b(\xi)$  can be expressed as

$$b(\xi) = B'_0 + B'_1w^1 + \dots + B'_{k-1}w^{k-1}, \quad (4.1.3)$$

where  $B'_i \in SP_p^m[w]$ . It may be noted that both residue field  $P_p^m[w]$  and subfield  $SP_p^m[w]$  are subspaces of  $P_p^n[w^k]$ . Various representations of  $P_p^n[w^k]$  are summarized in Table 4.1.1.

**Table 4.1.1 Various Representations of  $P_p^n[w^k]$**

a	Representation	Basis
$a_0 + a_1\xi + \dots + a_{r-1}\xi^{n-1}$ where $a_i \in GF(p)$	$a_0a_1\dots a_n$	Standard Basis over $GF(p)$
$a'_0 + a'_1w + \dots + a'_{k-1}w^{k-1}$ where $a'_i \in \text{Residue field } P_p^m[w]$	$a'_0a'_1\dots a'_{k-1}$	Ideal Basis over residue field $P_p^m[w]$
$a'_0 + a'_1w + \dots + a'_{k-1}w^{k-1}$ where $a'_i \in SP_p^m[w]$	$a'_0a'_1\dots a'_{k-1}$	Ideal Basis over $SP_p^m[w]$ .

*Example 4.1.1: Standard and Ideal Basis Representations of  $P_2^4[((1+\xi+\xi^2)^2)]$ :* Elements of residue field  $P_2^2[(1+\xi+\xi^2)]$  and  $SP_2^2[(1+\xi+\xi^2)]$  are given by the sets  $\{0, 1, \xi, 1+\xi\}$  and  $\{0, 1, \xi^2=\delta, 1+\xi^2=\delta^2\}$  respectively. The elements of  $P_2^4[((1+\xi+\xi^2)^2)]$  in all the three representations are given in Table 4.1.2. The ideal basis is given by the set  $\{1, (1+\xi+\xi^2)\}$ .

Group of unit structure of  $P_p^n[w^k]$  is given in Appendix D; it is given by the direct product of two groups  $G_{PRA}$  and  $G_{PRC}$ , where  $G_{PRA}$  is Abelian component group and  $G_{PRC}$  is cyclic component group. From (D.3) of Appendix D, any unit element can be written as product of two elements, one drawn from  $G_{PRC}$  and the other from  $G_{PRA}$ . The non-zero elements of the subring  $SP_p^m[w]$  gives all the elements of  $G_{PRC}$  (Lemma D.1 of Appendix D). Thus any unit element 'a' can be written as

$$a = bc, b \in SP_p^m[w] = G_{PRC}, c \in G_{PRA} \quad (4.1.4)$$

#### 4.1.2 Representations of $PGR(V^k, r)$

Definition and essential structural properties of Galois extension ring of  $P_p^n[w^k]$  of degree r, denoted by  $PGR(V^k, r)$ , where V represents residue field  $P_p^m[w(\xi)]$  with  $p^m$  elements, are given in Appendix D. This

Table 4.1.2 Elements of  $P_2^4[((1+\xi+\xi^2)^2)]$  in Different Representations

Binary vectors in the table represent polynomial over GF(2):

For example, (1011) represents polynomial  $1+\xi^2+\xi^3$

$\delta$  is a primitive element in  $SP_p^m[w]$

Standard Basis Representation	Ideal Basis Representation I	Ideal Basis Representation II
(0000)	(00)(00)	(0,0)
(1000)	(10)(00)	(1,0)
(0100)	(01)(00)	( $\delta^2, 1$ )
(1100)	(11)(00)	( $\delta, 1$ )
(0010)	(11)(10)	( $\delta, 0$ )
(1010)	(01)(10)	( $\delta^2, 0$ )
(0110)	(10)(10)	(1,1)
(1110)	(00)(10)	(0,1)
(0001)	(10)(11)	(1, $\delta$ )
(1001)	(00)(11)	(0, $\delta$ )
(0101)	(11)(11)	( $\delta, \delta^2$ )
(1101)	(01)(11)	( $\delta^2, \delta^2$ )
(0011)	(01)(01)	( $\delta^2, \delta$ )
(1011)	(11)(01)	( $\delta, \delta$ )
(0111)	(00)(01)	(0, $\delta^2$ )
(1111)	(10)(01)	(1, $\delta^2$ )

section gives representations of  $PGR(V^k, r)$  using the representations given in Section 4.1.1.  $PGR(V^k, r)$  contains elements of the form  $\sum_{i=0}^{r-1} a_i x^i$ ,  $a_i \in P_p^n[w^k]$ . The elements of  $PGR(V^k, r)$  can be viewed as module elements of length  $r$  over  $P_p^n[w^k]$ . But,  $P_p^n[w^k]$ , a local ring can be viewed as a vector space. We derive representations of  $PGR(V^k, r)$  using those of  $P_p^n[w^k]$ . The representations of  $P_p^n[w^k]$  given in Table 4.1 are made use of here to get representations of  $PGR(V^k, r)$  in terms of residue field  $PGR(V, r) \equiv GF(V^r)$ . (The homomorphism mapping  $\mu$  from  $P_p^n[w^k]$  to  $P_p^m[w]$  on the coordinates of  $PGR(V^k, r)$  yields residue field  $PGR(V, r) \equiv GF(V^r)$ ). Let  $\alpha = \alpha_0 + \alpha_1 x + \dots + \alpha_{r-1} x^{r-1} \in PGR(V^k, r)$ , where  $\alpha_i \in P_p^n[w^k]$ . Then by using ideal representation of  $P_p^n[w^k]$ ,  $\alpha$  can be written as

$$\alpha = \alpha_0 + \alpha_1 x + \dots + \alpha_{r-1} x^{r-1};$$

where  $\alpha_i = (\alpha_{i,0} + \alpha_{i,1} w + \dots + \alpha_{i,k-1} w^{k-1})$ ,  $\alpha_{i,j} \in P_p^m[w]$ ,  $j=0,1,\dots,k-1$ .

By expressing in terms of the basis  $\{1, w, \dots, w^{k-1}\}$ ,  $\alpha$  can also be written as

$$\alpha = \alpha'_0 + \alpha'_1 w + \dots + \alpha'_{k-1} w^{k-1},$$

where  $\alpha'_j = (\alpha_{0,j} + \alpha_{1,j} x + \dots + \alpha_{r-1,j} x^{r-1}) \in \text{Residue field } PGR(V, r) \equiv GF(V^r)$ . Thus  $PGR(V^k, r)$  can be considered as a vector space over residue field  $PGR(V, r)$ .

Similarly by using ideal representation over  $SP_p^m[w]$  we can have ideal basis representation over subfield  $SPGR(V, r)$ . Note that the ideal basis for  $P_p^n[w^k]$  is also a basis of  $PGR(V^k, r)$ . Various representations, arising out of vector space structure of  $PGR(V^k, r)$ , are given Table 4.1.2.

Table 4.1.2: Representations of  $PGR(V^k, r)$

$\alpha$	Representation	Basis
$\alpha_0 + \alpha_1 x + \dots + \alpha_{r-1} x^{r-1}$ where $\alpha_i \in P_p^n[w^k]$	$\alpha_0 \alpha_1 \dots \alpha_n$	Standard Basis over $P_p^n[w^k]$
$\alpha'_0 + \alpha'_1 w + \dots + \alpha'_{k-1} w^{k-1}$ where $\alpha'_i \in \text{Residue field } PGR(V, r)$	$\alpha'_0 \alpha'_1 \dots \alpha'_{k-1}$	Ideal Basis over residue field $PGR(V, r)$
$\alpha'_0 + \alpha'_1 w + \dots + \alpha'_{k-1} w^{k-1}$ where $\alpha'_i \in SPGR(V, r) = GF(V^r)$	$\alpha'_0 \alpha'_1 \dots \alpha'_{k-1}$	Ideal Basis over $SPGR(V, r)$ .

## 4.2 Trace Sequence Families

Definition of trace sequence families is similar to the one given in Chapter 3 except that, here the appropriate ring over which trace sequences are defined is  $PGR(V^k, r)$ . Relevant properties of trace functions over  $PGR(V^k, r)$ , given in Appendix D, are used. A family of sequences is defined associated with every unit element  $\alpha$  belonging to  $PGR(V^k, r)$ . The sequences are generated as the trace of successive powers of  $\alpha$ ; the multiplicative order of  $\alpha$  determines the period of the sequences. Since  $P_p^n[w^k]$  is also a local ring, a trace family includes sequences over its ideals. The sequences over the ideal isomorphic to  $P_p^{m\kappa}[w^\kappa]$ ,  $1 \leq \kappa \leq k$ , are denoted as  $(k-\kappa)^{th}$  level sequences, and, accordingly, there are totally  $k$  level sequence groups. A  $\kappa^{th}$  level sequence associated with a unit element  $a \in G_a$  of  $PGR^*(V^k, r)$ ,  $S^{a, \kappa} = \{s_i\}$  (isomorphic to a sequence over  $P_p^{m\kappa}[w^\kappa]$ ) is given by

$$s_i = \text{tr}_1^r(w^\kappa a \alpha^i); i \in Z_L, \quad (4.2.1)$$

where  $L$  is the period of  $\alpha$ . It is clear that the total number of sequences in the family is  $(V^r-1)/L$ .

An unit element  $\alpha$  is called as primitive if its multiplicative order is same as the order of  $G_c$ , the cyclic component group of  $PGR^*(V^k, r)$  (ie.  $V^r-1$ ). Lemma 4.2.1 gives nature of multiplicative orders of unit elements.

**Lemma 4.2.1:** The multiplicative order of any unit element  $u$  divides

$$p^{k-1}(V^r-1)$$

and hence period of the trace sequences is of the form  $p^t(V^r-1)^b$ ,  $0 \leq t \leq k-1$ ,  $b = 0$  or  $1$ .

**Proof:** From the direct product representation of  $PGR^*(V^k, r)$  (Appendix (D)), any unit element  $u$  can be written as  $u = A\alpha$ ; where  $A \in G_a$ ,  $\alpha \in G_c$ . It is sufficient to show that the multiplicative order of elements of  $G_a$  divides  $p^{k-1}$ , then the multiplicative order of  $u$  divides  $p^{k-1}(V^r-1)$  since the order of  $G_c$  is  $(V^r-1)$ . For finding the order of  $A$ , consider the representation of  $A$  ((D.5) of Appendix D); any element of  $G_a$  can be written as

$$A = (1 + wA'), \text{ where } A' \in PGR(V^{k-1}, r).$$

*Rising*  
Rising both the sides by  $p^{k-1}$ , yields  $A^{p^{k-1}} = (1 + wA')^{p^{k-1}} = (1 + w^{p^{k-1}}A'^{p^{k-1}})$ , since the characteristic of the ring is  $p$ . But  $w^{p^{k-1}}$  is equal to zero, since  $p^{k-1} \geq k$  and  $w^k = 0$  ( $w$  is a zero divisor).

Thus  $A^{p^{k-1}} = 1$  and hence multiplicative order of  $A$  divides  $p^{k-1}$ . Thus, period of trace sequences generated by unit elements of  $PGR(V^k, r)$  is of the form  $p^t(V^r-1)^b$ ,  $0 \leq t \leq k-1$ ,  $b = 0$  or  $1$ .  $\square$

From Lemma 4.2.1 it is clear that period of the trace sequences is always a multiple of  $V^r-1$ . When the

order of  $\alpha$  chosen for sequence generation is  $V^r-1$  (primitive element), resultant sequences are called  $m$ -sequences. The  $m$ -sequence families are discussed in next Section 4.3.

The trace sequence generated by an element  $\alpha$  satisfies a linear recursion, over  $P_p^n[w^k]$ , given by

$$s_j = -\sum_{i=0}^{r-1} c_i s_{j-r+i} ; c_i \in P_p^n[w^k], j = r, r+1, \dots$$

The corresponding connection polynomial  $c(d)$  is given by

$$C(d) = d^r + \sum_{i=0}^{r-1} c_i d^i ; c_i \in P_p^n[w^k],$$

which is the minimum polynomial  $m_\alpha(d)$  of degree  $r$  over  $P_p^n[w^k]$ . Thus  $C(d) = m_\alpha(d) = (d-\alpha)(d-\sigma(\alpha))\dots(d-\sigma^{r-1}(\alpha))$ .

### 4.3 Families of Maximal Length Sequences over $P_p^n[w^k]$

As in the case of  $m$ -sequences over  $Z_{2^k}$ , if a primitive element  $\alpha \in G_c$  is chosen for trace sequence generation, the resulting sequences are called maximal length sequences ( $m$ -sequences) over  $P_p^n[w^k]$ . The generation mechanism of  $m$ -sequences over  $P_p^n[w^k]$  is similar to that of  $Z_{2^k}$ . For every primitive element  $\alpha$ , a family of  $m$ -sequences ( $\mathcal{K}^\alpha$ ) is defined. They can be treated as minimal cyclic codes of length  $V^r-1$  over  $P_p^n[w^k]$ . The ring  $P_p^n[w^k]$  has totally  $k$  ideals and accordingly there are  $k$  level sequences. Sequences over an ideal isomorphic to  $P_p^n[w^\kappa]$ ,  $0 \leq \kappa \leq k$  are denoted as  $\kappa^{\text{th}}$  level sequences. A  $\kappa^{\text{th}}$  level  $m$ -sequence,  $S^{\kappa,A} = \{s_i\}$ , indexed by an element  $A \in \text{PGR}^*(V^{k-\kappa}, r)$ , is given by

$$s_i = \text{tr}_1^r(w^\kappa A \alpha^i), 0 \leq \kappa \leq k, i \in Z_L,$$

where  $L$  is the period of the sequences given by the multilicative order of  $\alpha$ ,  $V^r-1$ . The distinct  $\kappa^{\text{th}}$  level sequences are given by the set  $\{S^{\kappa,A}, A \in G_a \text{ of } \text{PGR}^*(V^{k-\kappa}, r)\}$ . It is convenient to use Ideal basis representation over  $\text{SPGR}(V, r)$  for  $A \in G_a$  of  $\text{PGR}^*(V^{k-\kappa}, r)$  to identify different  $m$ -sequences. Here after, we consider only zeroeth level sequences, since  $\kappa^{\text{th}}$  sequences,  $\kappa > 0$ , are isomorphic to zeroeth level sequences of ring  $P_p^n[w^{k-\kappa}]$ . From (D.5) of Appendix D, any element  $A$  of  $G_a$  of  $\text{PGR}^*(V^k, r)$  can be written as  $(1+wA'), A' \in \text{PGR}(V^{k-1}, r)$ . Now by using ideal representation over  $\text{SPGR}(V, r)$  of  $A'$ ,  $A$  can be written as

$$A = 1 + w(A'_0 + wA'_1 + \dots + w^{k-2}A'_{k-1}), \quad (4.3.1)$$

where  $A'_j \in \text{SPGR}(V, r)$ . Hence a zeroeth level sequence,  $S^A = \{s_i\}$ , associated with an element  $A \in \text{PGR}^*(V^k, r)$  is given by  $s_i = \text{tr}_1^r(A \alpha^i) ; i = 0, 1, \dots, L-1$ .  $s_i = (s_{i,0}, s_{i,1}, \dots, s_{i,k-1})$  in ideal basis representation over  $\text{SP}_p^m[w]$  is then given by



$$s_{i,j} = \text{tr}_1^r(A'_{j-1} \alpha^i), 0 \leq j < k, \text{ with } A'_{-1} = 1. \quad (4.3.2)$$

For every  $A \in G_a$  of  $\text{PGR}^*(V^k, r)$ , we have a distinct sequence. Thus there are exactly  $V^{r(k-1)}$  zeroth level sequences. The sequences  $\{s_{i,j} : i \in \mathbb{Z}_L\} = S_j^A, j = 0 \leq j < k$  are called as component sequences of  $S^A$ .

Following definition of rank number of an element  $A$  of  $G_a \in \text{PGR}^*(V^k, r)$  is useful in stating correlation properties of  $m$ -sequences.

**Definition 4.3.1:** (Rank number ( $\mathcal{R}\mathcal{A}(a)$ ) of an element  $\alpha \in \text{PGR}(V^k, r)$  over  $\text{SPGR}(V, r)$ ). Consider the ideal basis representation of  $\alpha$  over  $\text{SPGR}(V, r) : \alpha = \alpha'_0 + \alpha'_1 w + \dots + \alpha'_{k-1} w^{k-1}$ , where  $\alpha'_j = (\alpha_{0,j} + \alpha_{1,j} x + \dots + \alpha_{r-1,j} x^{r-1}) \in \text{SPGR}(V, r), 0 \leq j < r, \alpha_{i,j} \in \text{SP}_p^m[w], 0 \leq i < k$ . Let  $M_\alpha$  be a  $r \times k$  matrix over  $\text{SP}_p^m[w]$  whose  $i, j^{\text{th}}$  element is given by  $\alpha_{i,j}$ . Then  $\mathcal{R}\mathcal{A}(a)$ , the rank number of  $\alpha$ , is defined as the rank of the matrix  $M_\alpha$ . It is also given by the rank of  $\text{SPGR}(V, r)$  elements over  $\text{SP}_p^m[w]$  present in  $\alpha$ .

*Example 4.3.1:* Zeroth level  $m$ -sequences over  $P_2^2[\xi^2]$  of period 7 generated by  $\alpha \in G_c$  of  $\text{PGR}(V^2, 3)$ ,  $V = \text{GF}(2)$ , such that  $1 + \alpha = \alpha^3$ , are given in Table 4.3.1. Elements of  $P_2^2[\xi^2]$  are represented by 2-tuples over  $\text{GF}(2)$ , for example symbol (11) represents  $1 + \xi$ .

### 4.3.1 Number of Distinct Families of $m$ -sequences

Two  $\mathcal{A}$  families are cyclically equivalent if the sequences of one family is obtained as the cyclic shift of sequences in the other. The number of distinct  $\mathcal{A}$  families depends on the number of primitive unit elements of  $G_c$ . There are exactly  $\phi(V^r - 1)$  unit elements in  $G_c$  whose period is  $V^r - 1$ , where  $\phi$  is the Euler's

Table 4.3.1  $m$ -sequences of Example 4.3.1

$A$	$S^A$	$\mathcal{R}\mathcal{A}(A)$
$[(10) + (00) + \alpha(00)\alpha^2]$	(00)(00)(10)(00)(10)(10)(10)	1
$[(01) + (00) + \alpha(00)\alpha^2]$	(00)(00)(01)(00)(01)(01)(01)	1
$[(10) + (11) + \alpha(00)\alpha^2]$	(00)(11)(10)(11)(01)(01)(10)	2
$[(01) + (11) + \alpha(00)\alpha^2]$	(00)(11)(01)(11)(10)(10)(01)	2
$[(10) + (00) + \alpha(11)\alpha^2]$	(11)(00)(01)(11)(01)(10)(10)	2
$[(01) + (00) + \alpha(11)\alpha^2]$	(11)(00)(10)(11)(10)(01)(01)	2
$[(10) + (11) + \alpha(11)\alpha^2]$	(11)(11)(01)(00)(10)(01)(10)	2
$[(01) + (11) + \alpha(11)\alpha^2]$	(11)(11)(10)(00)(01)(10)(01)	2

$\phi$  function;  $\phi(x)$  is equal to the number of integers less than or equal to  $x$  and relatively prime to  $x$ . Since the trace is invariant under the automorphisms,  $\alpha$  and  $\sigma(\alpha)$  yields same  $\mathcal{K}$  family. Thus  $\mathcal{K}$  families  $\mathcal{K}^{\sigma^i(\alpha)}$ ,  $i=0,1,\dots,r-1$ , are all cyclically equivalent. Thus there are exactly  $\phi(2^r-1)/r$  distinct  $\mathcal{K}$  families.

#### 4.4 Hamming Correlation Properties of $m$ -sequences over $P_p^n[w^k]$

This section gives Hamming autocorrelation properties of zeroth level  $m$ -sequences over  $P_p^n[w^k]$ . Throughout this section ideal basis representation of  $P_p^n[w^k]$  over  $SP_p^m[w]$  is assumed. We make use of Hamming correlation definition and Hamming correlation transform ( $\mathcal{K}^H$ ) definition given in Section 2.1. Following definition is useful in calculating  $\mathcal{K}^H$  of sequences over  $P_p^n[w^k]$ .

**Definition 4.4.1:**  $\mathcal{K}_S A(s)$ : Given an  $m$ -sequence  $S^A$  over  $P_p^n[w^k]$ ,  $\mathcal{K}_S A(s)$  is defined as the number of occurrences of the element  $s$  in the sequences  $S^A$  with in one period length.

Using Definition 4.4.1, Hamming correlation transform of  $S^A$  turns out be

$$\mathcal{K}(S^A) = \mathcal{K}_S A(0) \quad (4.4.1)$$

Lemma 4.4.1 gives an expression for computing Hamming correlation between two sequences over  $P_p^n[w^k]$  using Definition 4.4.1.

**Lemma 4.4.1:** Let  $S^A$  and  $S^B$  be two sequences over  $P_p^n[w^k]$ , then Hamming correlation between  $S^A$  and  $S^B$ ,  $H_{AB}(\tau)$  is given by

$$H_{AB}(\tau) = \mathcal{K}_D \tau(0^k), \text{ where } D^\tau = S^A - S^B \alpha^\tau.$$

**Proof:** Result follows from (2.1.15) and (4.4.1).

Hamming correlation computations make use of vector space structure of  $P_p^n[w^k]$  and properties of  $m$ -sequences over finite field. Relevant properties of  $m$ -sequences over finite field are given below.

##### 4.4.1 Properties of $m$ -sequences over Finite Field

**P.1** Let  $B = \{b_i, i \in Z_{V^r}\}$  be an  $m$ -sequence over a field  $GF(V)$  of period  $V^r-1$ , and let  $Rt_i, i \in Z_{V^r}$ , be a  $r$ -tuple given by  $(b_i, b_{i+1}, \dots, b_{i+r-1})$ , then set of  $r$ -tuples  $\{Rt_i, i \in Z_{V^r}\}$  are distinct and the set accounts for all  $r$ -tuples over  $GF(V)$  barring an all zero tuple.

**P.2**  $V^r-1$  shifts of  $m$ -sequences are closed under point wise addition, ie. set of all  $V^r-1$  shift  $m$ -sequences and an all zero sequence forms an Abelian group under point wise addition.

#### 4.4.2 Hamming Autocorrelation Properties of m-sequences over $P_p^n[w^k]$ .

Fact that component sequences over  $P_p^n[w^k]$  are m-sequences over subfield  $SP_p^m[w] = GF(V)$  and the linear property of m-sequences over  $P_p^n[w^k]$  are used in the computation of Hamming autocorrelation properties. Lemmas 4.4.2–4.4.5 establish autocorrelation properties of m-sequences over  $P_p^n[w^k]$ .

**Lemma 4.4.2:** P.2 is even true for m-sequences over  $P_p^n[w^k]$ .

**Proof:** Let  $S^A = \{s_i\}$  be an m-sequence associated with an element  $A \in PGR^*(V^k, r)$ . Then  $\tau^{th}$  shift of  $S^A$  is given by  $S^{A\alpha^\tau} = \{s'_i\}$  where  $s'_i = tr_1^r(A\alpha^{i+\tau})$ ,  $i \in Z_L$ . The pointwise difference of  $S^A$  and  $S^{A\alpha^\tau}$  is given by  $(S^A - S^{A\alpha^\tau}) = \{s''_i\}$ ;  $s''_i = tr_1^r(A\alpha^i(1-\alpha^\tau))$ ,  $i \in Z_L$ . Since  $\{G_c, 0\}$  is the subfield  $SPGR(V, r) = GF(V^r)$ ,  $(1-\alpha^\tau) \in G_c$ . Thus  $(S^A - S^{A\alpha^\tau})$  is equal to  $\tau'$  shift of  $S^A$  ( $\tau' = 1-\alpha^\tau$ ). This implies that various shifts of  $S^A$  forms an Abelian group under pointwise subtraction.  $\square$

**Lemma 4.4.3:** Let  $S^A = \{s_i\}$  be an m-sequence over  $P_p^n[w^k]$ , and  $\mathcal{R}(A)$  be  $\rho$ , then set of column vectors derived from  $S^A$ , over  $SPGR(V, r)$ ,  $\{s_{i,0}\}^T \{s_{i,1}\}^T, \dots, \{s_{i,k-1}\}^T$ ,  $i = i_1, i_1+1, \dots, i_1+\rho-1$ ,  $0 \leq i_1 \leq V^r-2$ , have a column rank  $\rho$ .

**Proof:** The ideal basis component elements of  $A$ ,  $\{1, A'_0, A'_1, \dots, A'_{k-1}\}$  (refer (4.3.1)) have rank  $\rho$  over  $SPGR(V, r)$ , since  $\mathcal{R}(A)$  is  $\rho$ . The fact that the trace function is a linear function from  $SPGR(V, r)$  to  $SP_p^m[w]$  implies that the column rank of the set has to be less than or equal to  $\rho$ . If the column rank is less than  $\rho$ , say  $\rho'$ , then  $\{s_{i,\rho}\}$  can be written as linear sum of  $\rho'$  linearly independent vectors. This means that  $s_{i,\rho} = \sum_{j=1}^{\rho'} L_j s_{i,j}$ , for all  $i$ , where  $L_j \in SP_p^m[w]$  and  $\{\{s_{i,j}\}, j=1 \dots \rho'\}$  are linearly independent column sequences. Then by using (4.3.2)  $s_{i,\rho}$  can be written as  $tr_1^r(A'_{\rho-1} \alpha^i) = tr_1^r(\sum_{j=1}^{\rho'} L_j A'_{j-1} \alpha^i)$ . This equation for  $i=0$  implies that  $\mathcal{R}(A)$  is  $\rho'$  contradicting the fact that  $\mathcal{R}(A)$  is  $\rho$ . Hence the column rank has to be  $\rho$ .  $\square$

**Lemma 4.4.4:** For any m-sequence over  $P_p^n[w^k]$  of period  $V^r-1$ ,  $S^A = \{s_i\}$ , with  $\mathcal{R}(A)$  equal to  $r$ ,

- Component sequences  $\{\{s_{i,j}\}; j = 0, \dots, r-1\}$  are linearly independent over  $SP_p^m[w]$ .
- No element  $s_i$  is identically equal to zero.
- All the elements  $\{s_i\}$  are distinct and appear only once in one period. ie.  $\mathcal{N}_S A(s) = 1$  for all non zero  $s$ .
- The set of  $r$ -tuples,  $\{s_{i,j}, j=0, \dots, r-1; i \in Z_{V^r-1}\}$  accounts for all  $r$ -tuples over  $SP_p^m[w]$ .

**Proof:** The result a) follows from Lemma 4.4.3. The result b) is true, other wise  $s_{i_1} = 0$  implies that the vectors  $\{\{s_{i_0}\}^T, \{s_{i_1}\}^T, \dots, \{s_{i_{r-1}}\}^T, i = i_1, i_1+1, \dots, i_1+r-1\}$  have rank  $< r$ , contradicting Lemma 4.4.3. If any two elements of  $S^A$  are identical, say  $s_{i_1}$  and  $s_{i_2}$  then from Lemma 4.4.2 the pointwise difference of two sequences  $S^A \alpha^{i_1}$  and  $S^A \alpha^{i_2}$ ,  $(S^A \alpha^{i_1} - S^A \alpha^{i_2})$ , yield an  $m$ -sequence which has a zero element thus contradicting b). Hence c) is true. The result d) follows from c) since the period of  $S^A$  is  $V^r-1$  and there are only  $V^r-1$  non zero  $r$ -tuples over  $SP_p^m[w]$ .  $\square$

**Lemma 4.4.5:** Let  $S^A$  be an  $m$ -sequence over  $P_p^n[w^k]$  of period  $V^r-1$ , with  $\mathcal{RA}(A) = \rho$ . Then

$$\mathcal{K}_S A(0^k) = V^{r-\rho}-1, \text{ and}$$

$$\mathcal{K}_S A(s) = V^{r-\rho} \text{ for } s \neq 0^k.$$

**Proof:** Consider ideal basis representation of elements of  $S^A$ , then for  $s \in S^A$ ,  $\mathcal{K}_S A(s) = \mathcal{K}_S A(s'_0, s'_1, \dots, s'_{k-1})$ , where  $s'_j \in SP_p^m[w]$ . From Lemma 4.4.3, we know that column rank of  $\{s_{i,j}\}$  is  $\rho$  and let  $\{s_{i,j_1}\}, \{s_{i,j_2}\}, \dots, \{s_{i,j_{\rho_r}}\}$  be linearly independent component sequences over  $SP_p^m[w]$ . Then  $\mathcal{K}_S A(s'_0, s'_1, \dots, s'_{k-1}) = \mathcal{K}_S A(s'_{j_1}, s'_{j_2}, \dots, s'_{j_{\rho}})$ , since rest of the bits in  $s$  are linearly related to  $(s'_{j_1}, s'_{j_2}, \dots, s'_{j_{\rho}})$ .  $\mathcal{RA}(A)$  cannot exceed  $r$  since  $S^A$  satisfies a linear recurrence of order  $r$ . Now consider a sequence  $\hat{S}^A = \{t_i\}$  whose component sequences in positions  $j_1, j_2, \dots, j_{\rho}$  are same as those of  $S^A$ , with  $\mathcal{RA}(\hat{A}') = r$ ;  $\hat{A}'_{j_1} = A'_{j_1}$ ,  $\hat{A}'_{j_2} = A'_{j_2}, \dots, \hat{A}'_{j_r} = A'_{j_r}$ . Then there are exactly  $V^{r-r'} k$  tuples  $(t'_0, t'_1, \dots, t'_{k-1})$  in  $\hat{S}^A$  such that  $(s'_{j_1}, s'_{j_2}, \dots, s'_{j_{\rho}}) = (t'_{j_1}, t'_{j_2}, \dots, t'_{j_{\rho}})$ . We have from Lemma 4.4.4 (Part 4)  $\mathcal{K}_S A'(t) = 0$  if  $t = 0^k$  and  $\mathcal{K}_S A'(t) = 1$  if  $t \neq 0^k$ . Hence  $\mathcal{K}_S A(s) = V^{r-\rho}-1$  if  $s=0^k$  and  $\mathcal{K}_S A(s) = V^{r-\rho}$  if  $s \neq 0^k$ .  $\square$

**Theorem 4.4.1:** Let  $S^A$  be an  $m$ -sequence over  $P_p^n[w^k]$ , with  $\mathcal{RA}(A) = \rho$ , of period  $V^r-1$ . Then

$$\begin{aligned} H_{AA}(\tau) &= V^r-1 \text{ if } \tau = 0 \\ &= V^{r-\rho}-1 \text{ if } \tau \neq 0. \end{aligned}$$

**Proof:** The case of  $\tau = 0$  is obvious. The case of  $\tau \neq 0$  follows from Lemmas 4.4.1 and 4.4.5.  $\square$

## 4.5 Sets of Frequency Hopping Patterns Derived from $m$ -sequences over $P_p^n[w^k]$

Associated with every  $m$ -sequence  $S^A$ , we construct a family of sequences which can be used to construct frequency hopping patterns. The number of sequences in a family depends on the number of distinct elements of  $P_p^n[w^k]$  occurring in  $S^A$ . Families are optimal in the sense that they meet Lempel and Greenberger bound on  $H_{\max}$  (Theorem 2.5.4). We give a definition for number of distinct elements in  $S^A$ .

**Definition 4.5.1:** Trace Image of  $S^A$ : It is defined as the set of distinct elements of the  $m$ -sequence  $S^A$ . The cardinality of the set is given by  $V^\rho$ , where  $\rho$  is the rank number of  $A$ . If  $A = 1 + w(A'_0 + wA'_1 + \dots + w^{k-2}A'_{k-1}) \in G_a$  of  $\text{PGR}^*(V^k, r)$ , and  $j_1, j_2, \dots, j_\rho$ ;  $j_i \in (0, 1, \dots, k-1)$  be the linearly independent positions in the ideal representation of  $A$ , then the Trace Image of  $S^A$  is given by the set

$$\{w^{j_1}a_{j_1} + w^{j_2}a_{j_2} + \dots + w^{j_\rho}a_{j_\rho} + w^{j_{\rho+1}}a_{j_{\rho+1}} + \dots + w^{j_{k-1}}a_{j_{k-1}}\}$$

where each  $a_{j_1}, a_{j_2}, \dots, a_{j_\rho}$  takes all values from  $\text{SP}_p^m[w]$  and  $a_{j_{\rho+1}}, \dots, a_{j_{k-1}}$  are linearly related to  $a_{j_1}, a_{j_2}, \dots, a_{j_\rho}$ ; the linear relation depends on  $A$ .

#### 4.5.1 Optimal Families of Sequences over $P_p^n[w^k]$

Let  $S^A = \{s_i\}$  be an  $m$ -sequence over  $P_p^n[w^k]$ , then for every  $\gamma \in \text{Trace image of } S^A$ , we define a sequence  $S^A(\gamma)$  given by  $\{s_i + \gamma, i \in \mathbb{Z}_{V^{r-1}}\}$ . Since the cardinality of trace image of  $S^A$  is  $V^\rho$ , we have  $V^\rho$  such sequences. Then a family of  $V^\rho$  sequences associated with  $S^A$  is given by the set of sequences  $\{S^A(\gamma), \gamma \in \text{Trace image of } S^A\}$ . We denote such a family by  $\mathcal{K}(A)$ .

**Theorem 4.5.1:** Hamming correlation between any two sequences  $S^A(\gamma_1)$  and  $S^A(\gamma_2)$  belonging to the family  $\mathcal{K}(A)$ , is given by

$$\begin{aligned} H_{\gamma_1\gamma_2}(0) &= V^r - 1 \text{ whenever } \gamma_1 = \gamma_2, \\ H_{\gamma_1\gamma_2}(\tau) &= V^{r-\rho} - 1 \text{ whenever } \gamma_1 = \gamma_2 \text{ and } \tau \neq 0, \\ H_{\gamma_1\gamma_2}(0) &= 0 \text{ whenever } \gamma_1 \neq \gamma_2, \\ H_{\gamma_1\gamma_2}(\tau) &= V^{r-\rho} \text{ whenever } \gamma_1 \neq \gamma_2 \text{ and } \tau \neq 0, \end{aligned}$$

Hence the family  $\mathcal{K}(A)$  satisfies Lempel and Greenberger bound on  $H_{\max}$ .

**Proof:** First two results follow from Theorem 4.4.1. Let  $\gamma_1 \neq \gamma_2$ , If  $\tau = 0$ , then from Lemma 4.4.1 and Lemma 4.4.2,  $H_{\gamma_1\gamma_2}(0)$  is given by  $\mathcal{K}_D(0^k)$ , where  $D = (S^A(\gamma_1) - S^A(\gamma_2))$  which is a sequence with each element  $\gamma_1 - \gamma_2 \neq 0$ . Thus  $H_{\gamma_1\gamma_2}(0)$  is zero. Similarly, if  $\tau \neq 0$ ,  $H_{\gamma_1\gamma_2}(\tau)$  is given by  $\mathcal{K}_D(0^k)$ , where  $D = S^A(\gamma_1) - S^A\alpha^\tau(\gamma_2)$ ;  $-$  represents pointwise subtraction.  $\mathcal{K}_D(0^k)$  is same as  $\mathcal{K}_D(\gamma_1 - \gamma_2)$ , where  $D' = S^{A(1-\alpha^\tau)}$  which is also an  $m$ -sequence. Then the result follows from Lemma 4.4.5. From equations (2.5.12) and (2.5.13) it is clear that  $\mathcal{K}(A)$  is optimal.  $\square$

Thus we have optimal families of sequences over  $P_p^n[w^k]$ . Next we give a construction of families frequency hopping patterns from  $\mathcal{K}(A)$

### 4.5.2 Frequency Hopping Patterns from $\mathcal{K}(A)$

Frequency hopping patterns are derived from sequences  $P_p^n[w^k]$  by a mapping from  $P_p^n[w^k]$  to frequency library. Each symbol  $a$  in the ring  $P_p^n[w^k]$  is associated with a distinct frequency belonging to the frequency library. Schematic diagram of generating frequency hopping patterns from sequences over  $P_p^n[w^k]$  is given in Fig 4.5.1. Basis selector chooses linearly independent component sequences of  $S^A$ .

### 4.5.3 Number of Families of Frequency Hopping Patterns

Corresponding to each  $m$ -sequence  $S^A$ , we have a family of hopping patterns derived from  $\mathcal{K}(A)$ . From the construction of  $\mathcal{K}(A)$  it is clear that size and properties of  $\mathcal{K}(A)$  depend  $\mathcal{R}\mathcal{K}(A)$ . Thus number of frequency hopping families of any specified size depends on rank number distribution of zeroth level  $m$ -sequences. Let  $\#(r, \rho)$  be number of zeroth level  $m$ -sequences  $S^A$  of period  $V^r - 1$  such that  $\mathcal{R}\mathcal{K}(A)$  equal to  $\rho$ . All these  $m$ -sequences  $S^A$  such that  $\mathcal{R}\mathcal{K}(A) = r$ , result in frequency hopping family of size  $V^\rho$ . From Section 4.3.1, we know that there are  $E(r)$  number of distinct  $\mathcal{K}$  families of period  $V^r - 1$ ;  $E(r) = \phi(V^r - 1)/r$ ;  $\phi$  is the Euler's  $\phi$  function. Thus number of families of frequency hopping patterns of size  $V^\rho$  derived from zeroth level sequences is given by  $\#(r, \rho)E(r)$ . Lemma 4.5.1 and Lemma 4.5.2 gives an expression for computing  $\#(r, \rho)$  and Table 4.5.3 gives number of frequency hopping families derived from zeroth level  $m$ -sequences.

**Lemma 4.5.1:**  $\#(r, \rho)$  is equal to number of  $r$  by  $r$  matrices over  $GF(V)$  of rank  $\rho$  with a condition that first column is given by  $(1, 0, \dots, 0)^T$ , where  $T$  stands for transpose.

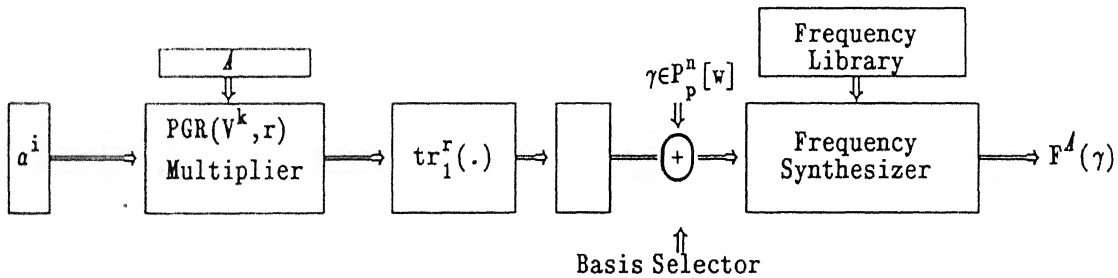


Fig 4.5.1 Schematic Diagram of Generation of Frequency Hopping Patterns using  $m$ -sequences over  $P_p^n[w^k]$

**Proof:** From (4.3.1), set of all zeroth level sequences are given by

$$\{S^A, A = 1 + w(A'_0 + wA'_1 + \dots + w^{k-2}A'_{k-1}), \text{ for all } A'_j \in \text{SPGR}(V, r)\}.$$

Then  $\#(r, \rho)$  is given by number of  $A$  such that  $\mathcal{RA}(A)$  equal to  $\rho$ . Result then follows from the definition of the rank number.  $\square$

**Lemma 4.5.2:**  $\#(r, \rho)$  is given by

$$((V^r - V^2) \dots (V^r - V^{\rho-1})) \left\{ \sum_{j=1}^{r-1} \prod_{m=1}^{r-\rho} V^{f_j^{(m)}} \right\},$$

where  $j^{(m)}, m = 1, \dots, \rho-1$  are chosen positions and  $\hat{j}^{(n)}, n = 1, \dots, r-\rho$ , are nonchosen positions in  $j^{\text{th}}$  combination of  $\begin{bmatrix} r-1 \\ \rho-1 \end{bmatrix}$ ,  $j^{(m)}, \hat{j}^{(n)} \in (1, \dots, \rho-1)$ , and  $f_j^{(m)}, m = 1, \dots, r-\rho$ , is the number of chosen positions  $j^{(i)}$  such that  $j^{(i)}$  is less than  $\hat{j}^{(m)}$ .

**Proof:** Let  $j^{(m)}, \hat{j}^{(m)}$ , and  $f_j^{(m)}$  are assumed in the statement of the Lemma. We count distinct matrices of rank  $\rho$  with first column given by  $(1, 0, \dots, 0)^T$  by giving a method of constructing such matrices. Since first column of the matrix is fixed, each matrix is formed by selecting  $\rho-1$  other linearly independent column positions among  $r-1$  remaining columns to make a matrix of rank  $\rho$ . This choice of linearly independent positions can be done in  $\begin{bmatrix} r-1 \\ \rho-1 \end{bmatrix}$  ways. Consider a  $j^{\text{th}}$  combination of  $\begin{bmatrix} r-1 \\ \rho-1 \end{bmatrix}$ . We select independent column positions as chosen positions  $j^{(m)}, m = 1, \dots, \rho-1$  and dependent column positions as nonchosen positions  $\hat{j}^{(m)}, m = 1, \dots, r-\rho$ . These  $\rho-1$  independent column positions can be filled by vectors over  $\text{GF}(V)$  in  $(V^r - V^2) \dots (V^r - V^{\rho-1})$  different ways. For each such configuration, dependent columns are filled with vectors as follows. Each dependent column position,  $\hat{j}^{(m)}$  is filled by taking linear combinations of vectors in independent column positions  $j^{(i)}$  such that  $j^{(i)} < \hat{j}^{(m)}$ . This way, we avoid taking linear sums of independent columns  $j^{(i)}$  such that  $j^{(i)} > \hat{j}^{(m)}$  in filling dependent column positions. This will not affect counting of distinct matrices as explained as follows: If in a matrix,  $\hat{j}^{(m)}$  is formed as a linear sum of chosen position say  $j^{(i)}$  such that  $j^{(i)} > \hat{j}^{(m)}$ , then this matrix is also counted in  $j^{\text{th}}$  combination of  $\begin{bmatrix} r-1 \\ \rho-1 \end{bmatrix}$  whose chosen positions include  $\hat{j}^{(m)}$  and all chosen positions of  $j^{\text{th}}$  combination except  $j^{(i)}$ . Thus with the method above we would be counting only distinct matrices. Hence the number of dependent vectors possible for column  $\hat{j}^{(m)}$  is  $V^{f_j^{(m)}}$ . Repeating this for all nonchosen positions, for  $j^{\text{th}}$  combination, dependent positions can be filled up in  $\prod_{m=1}^{r-\rho} V^{f_j^{(m)}}$  different ways. Thus for  $j^{\text{th}}$  combination number of matrices possible is  $(V^r - V^2) \dots (V^r - V^{\rho-1}) \prod_{m=1}^{r-\rho} V^{f_j^{(m)}}$ . Summing over all the combinations yields the result.  $\square$

Weight distribution of zeroth level  $m$ -sequences is computed from rank number distributions since weight structure of an  $m$ -sequence  $S^A$  is completely determined from  $\mathcal{RA}(A)$  (Lemma 4.4.5)

Table 4.5.1 gives the weight distribution. Table 4.5.2 lists  $\#(r, \rho)$  for  $r$  equal to 2, 3, 4, 5, 6.

Table 4.5.1 Weight Distribution of Zeroth Level  $m$ -sequences

$\rho$	Weight Distribution		Number of Sequences
	$\mathcal{N}(0^k)$	$\mathcal{N}(s \neq 0^k)$	
1	$V^{r-1}-1$	$V^{r-1}$	$\#(r, 1)$
2	$V^{r-2}-1$	$V^{r-2}$	$\#(r, 2)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\rho$	$V^{r-\rho}-1$	$V^{r-\rho}$	$\#(r, \rho)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$r$	0	1	$\#(r, r)$

where  $\mathcal{N}(s)$  means number of occurrences of  $s$  in a sequence

Table 4.5.2  $\#(r, \rho)$  for  $r = 2, 3, 4, 5, 6$

$\rho$	$\#(2, \rho)$	$\#(3, \rho)$	$\#(4, \rho)$	$\#(5, \rho)$	$\#(6, \rho)$
1.	2	4	8	16	32
2.	2	36	392	3600	30752
3.		24	2352	17600	4612800
4.			1344	604800	129158400
5.				322560	619960320
6.					319979520
$\Sigma \#(r, \rho) =$	4	64	4096	1048576	1073741824

$\#(r, \rho)$  is equal to number of  $r$  by  $r$  matrices over  $GF(V)$  of rank  $\rho$

with a condition that first column is given by  $(1, 0, \dots, 0)^T$ ,

where  $T$  stands for transpose



*Example 4.5.1:* Family of frequency hopping patterns of length 7 derived from m-sequences over  $P_2^3[\xi^3]$ .

Sequences are generated by  $\alpha$  such that  $\alpha^3 = \alpha + 1$ ,  $\alpha \in \text{PGR}(V^3, 3)$ , where  $V = \text{GF}(2)$ . Patterns are constructed from an m-sequence  $S^A$ ,  $A = (1) + (\xi^2)\alpha + (\xi)\alpha^2$ ;  $S^A$  is given by:

$$S^A = \{(\xi), (\xi^2), (1+\xi), (\xi+\xi^2), (1+\xi+\xi^2), (1+\xi^2), (1)\}.$$

Patterns of the family  $\mathcal{M}(1) + (\xi^2)\alpha + (\xi)\alpha^2$  are given in Table 4.5.4. Pattern symbols are represented by decimal numbers in the range (0–7);  $a(\xi)$  of  $P_2^3[\xi^3]$  is represented by  $a(2)$ .

**Table 4.5.3 Number of Frequency Hopping Families**

Obtained from Zeroth Level m-sequences over  $P_p^n[w^r]$  of Period  $V^r - 1$

Size	Number of families
$V$	$\#(r, 1)E(r)$
$V^2$	$\#(r, 2)E(r)$
$\vdots$	$\vdots$
$V^\rho$	$\#(r, \rho)E(r)$
$\vdots$	$\vdots$
$V^r$	$\#(r, r)E(r)$

$$E(r) = \phi(V^r - 1)/r$$

**Table 4.5.4 Frequency Patterns of Family  $\mathcal{M}(1) + (\xi^2)\alpha + (\xi)\alpha^2$  (Example 4.5.1)**

$\gamma$	$S^A(\gamma)$
0	2 4 3 6 7 5 1
1	3 5 2 7 6 4 0
$\xi$	0 6 1 4 5 7 3
$1+\xi$	1 7 0 5 4 6 2
$\xi^2$	6 0 7 2 3 1 5
$1+\xi^2$	7 1 6 3 2 0 4
$\xi+\xi^2$	4 2 5 0 1 3 7
$1+\xi+\xi^2$	5 3 4 1 0 2 6

## 4.6 m-sequences Having Ideal Block Inner-product Autocorrelations.

From Table 2.2.1, it is clear that  $P_p^n[w^k]$  is a matched structure to signal set for block inner-product correlations. the vector space structure of  $P_p^n[w^k]$  is responsible for such a matching. We shall consider here special case of  $P_p^n[w^k]$  where  $w$  is of degree 1, which implies that residue field is  $GF(p)$ . Hence throughout this section  $V$ , the order of the residue field is  $p$ .

### 4.6.1 Block $p$ -phase Sequences from $P_p^n[w^k]$ Sequences

Here the mapping  $\phi$  is from  $P_p^n[w^k]$  to  $C^k$ ,  $k$ -dimension complex space and is given by

$$\phi^B(A) = \phi^B(a_0 a_1 \dots a_{k-1}) = \phi(a_0) \phi(a_1) \dots \phi(a_{k-1}) \quad (4.6.1)$$

where  $\phi$  is inner-product mapping from  $GF(p)$  to  $p^{\text{th}}$  root of unity given by

$$\phi(a) = \exp\left(\frac{\omega 2 \pi a}{p}\right). \quad (4.6.2)$$

If  $S^A = \{s_i\}$  is a sequence over  $P_p^n[w^k]$ , the block  $p$ -phase sequence  $\{s_i^B\}$  is obtained by the mapping  $\phi$ , given by

$$s_i^B = \phi^B(s_i).$$

The block inner-product correlation transform of  $S^A$  is given by

$$\kappa^B(S^A) = \sum_{i=0}^{L-1} \phi^B(s_i) \quad (4.6.3)$$

Then autocorrelation function  $C_{AA}(\tau)$  is given by

$$C_{AA}(\tau) = \kappa^B(S^A - T^\tau(S^A)) \quad (4.6.4)$$

### 4.6.2 Block Inner-product Autocorrelations of $m$ -sequences over $P_p^n[w^k]$

In this subsection we compute autocorrelation properties of block  $p$ -phase sequences derived from  $m$ -sequences over  $P_p^n[w^k]$ .

**Lemma 4.6.1:** Let  $S^A$  be an  $m$ -sequence over  $P_p^n[w^k]$ , then  $\kappa^B(S^A)$  is given by the sum of inner-product correlation transforms of component sequences of  $S^A$ .

**Proof:** Follows from (2.1.19).  $\square$

**Theorem 4.6.1:** Let  $S^A$  be an  $m$ -sequences over  $P_p^n[w^k]$  with component sequences being identically not equal to zero, then block IP autocorrelations of  $S^A$  is given by

$$C_{AA}(\tau) = k(p^r-1) \text{ whenever } \tau=0$$

$$C_{AA}(\tau) = -k \text{ whenever } \tau \neq 0$$

**Proof:** From Theorem 2.2.1 and Lemma 4.6.1, we have

$$C_{AA}^{BIP}(\tau) = \kappa^{BIP}(S^A - T^\tau(S^A)) = \sum_{j=1}^k \kappa^{IP}(S_j^A - T^\tau(S_j^A)).$$

For  $\tau = 0$ , the result is evident. Let  $\tau \neq 0$ . Since component sequences  $S_j^A$ ,  $1 \leq j \leq k$ , are nonzero  $m$ -sequences over  $GF(p)$  of period  $p^r-1$ ,  $\kappa^{IP}(S_j^A - T^\tau(S_j^A))$  is  $-1$ . Result then follows since no component sequence is identically a zero sequence.  $\square$

Thus we have sequences with ideal block inner-product autocorrelations. In the above construction we have considered the ring  $P_p^n[w^k]$  where degree of  $w(\xi)$  is one for simplicity. However the result holds good for rings where degree of  $w(\xi)$  is greater than one also. Komo [79] has constructed such block  $p$ -phase sequences using  $m$ -sequences over  $GF(p^r)$  having ideal block inner-product correlations. Here we have demonstrated similar construction over polynomial residue class rings.

## Chapter 5

### Controllable Large Linear Complexity Sequences over $Z_4$ and Local Residue Class Polynomial Rings

This chapter gives construction of non-linear families of sequences over residue class rings  $Z_4$  and  $P_p^n[w^k]$  with controllable large linear complexity (LC). The sequences in a family are not closed under pointwise ring addition. This implies that the linear complexity of sequences derived from a  $r^{\text{th}}$  degree Galois extension ring is always greater than  $r$  (corresponding linear sequences have LC less than or equal to  $r$ ). These sequences are of prime importance in secure communications where low LC of sequences renders system vulnerable to jamming attacks. The non-linear sequences over  $Z_4$  and  $P_p^n[w^k]$  derived here are employed to obtain quadriphase sequences and frequency hopping patterns respectively.

A procedure for obtaining controllable large LC sequences over finite fields, given by Siegenthaler and Forre [47], is generalized to residue class rings. The procedure uses generalized permutation polynomials over Galois extension rings. By using generalizations of permutation monomials, generalized GMW sequences (GGMW) are constructed. Generalized Blahut's theorem over finite rings given in Section 2.5.3 has been used for the computation of the LC of sequences.

The families of GGMW sequences over  $Z_4$  satisfy Welch bound on inner products with equality. However,  $\theta_{\max}$  deviates from optimal value of  $\sqrt{L}$ ;  $L$  being the period of the sequences. We have some computer results which suggest that the number of crosscorrelation values which deviate from optimal value of  $\sqrt{L}$  is small. The correlation transform of these sequences is same as those of  $m$ -sequences.

The chapter is organized as follows. Section 5.1 gives generalized permutation monomials over  $GR(4,r)$  and  $PGR(V^k,r)$ . Section 5.2 discusses a generalized procedure for constructing large LC sequences obtained from trace sequences using permutations on Galois extension rings. Families of GGMW sequences are defined in Section 5.3. Sections 5.4 and 5.5 give properties of GGMW sequences over  $Z_4$  and  $P_p^n[w^k]$  respectively.

#### 5.1 Permutations over $GR(4,r)$ and $PGR(V^k,r)$

Permutations on finite fields have polynomial representations while same is not true in the case of residue class finite rings [67,92]. Polynomial substitution,  $y \longrightarrow g(y)$  ( $g(y)$  is a polynomial of degree  $> 2$ )

cannot be a permutation on Galois rings due to the presence of zero divisors. In this section we use properties of  $GR(4,r)$  and  $PGR(V^k,r)$  to define permutations on respective Galois rings.

### 5.1.1 Permutations over $GR(4,r)$

We assume that the permutation  $P$  acts independently on different multiplicative groups of  $GR(4,r)$ . From P7 and P8 of Section 3.1, any element  $a \in GR(4,r)$  can be expressed as  $(2^i\beta\alpha)$ ; where  $i=0$  or  $1$ ,  $\beta \in G_a$  and  $\alpha \in G_c$ . Then permutation  $P$  is defined as follows:

$$\begin{aligned} P(a) &= P_1(\beta)P_2(\alpha) \text{ when } i = 0, \\ P(a) &= \beta P_3(\alpha) \text{ when } i = 1, \end{aligned} \quad (5.1.1)$$

where  $a = (2^i\beta\alpha)$  and  $P_1(\cdot)$  is a permutation on  $G_a$ ,  $P_2(\cdot)$  and  $P_3(\cdot)$  are permutations on  $G_c$ . Such a permutation  $P$  is identified by a triplet  $[P_1, P_2, P_3]$ . Permutation  $P$  is called as generalized permutation polynomial when permutations  $P_1, P_2, P_3$  are defined by polynomial substitutions. Two types of permutation monomials are considered.

**Monomial of the First type ( $\Psi_1$ ):** Here the permutation is defined as follows: For any  $a \in GR(4,r)$ ,  $a = 2^i a_u$ ;  $i=0$  or  $1$  and  $a_u$  is a unit element,  $\Psi_1^b$  is defined as

$$\Psi_1^b(a) = 2^i g(a) \quad (5.1.2)$$

where  $g(x)$  is a permutation monomial over group of units  $GR^*(4,r)$ .

**Lemma 5.1.1:** A monomial  $g(x) = x^b$ ,  $b$  an integer  $0 < b \leq 2(2^r-1)$ , is a permutation polynomial on  $GR^*(4,r)$ , group of units of  $GR(4,r)$ , if and only if

$$(b, 2^r-1) = 1 \text{ and } (b, 2) = 1,$$

where  $(d,f) = 1$  implies that  $d$  and  $f$  are relatively prime to each other.

**Proof:** Result follows from the structure of group of units  $GR^*(4,r)$ ; it is expressed as direct product of two groups  $G_a$  and  $G_c$ , where  $G_a$  is an Abelian group of order  $2^r$  and  $G_c$  is a cyclic group of order  $2^r-1$  (P6 of Section 3.1). The above conditions are necessary since  $G_c$  is a cyclic group of order  $2^r-1$  and  $G_a$  contains units of order 2 (refer (3.1.1)). Sufficiency can be easily seen.  $\square$

**Monomial of the Second type (Power Permutation Polynomials):**

Let  $b = b_0 + b_1 2 + \dots + b_{r-1} 2^{r-1}$ , be an integer such that  $0 < b \leq 2^r-1$ . Then by  $x \longrightarrow x^{\text{power}(b)}$ , we mean a substitution of the following kind:

$$a \longrightarrow (\sigma^0(a))^{b_0} (\sigma^1(a))^{b_1} \dots (\sigma^{r-1}(a))^{b_{r-1}}, \quad (5.1.3)$$

$b_i \in 0,1$  and  $\sigma^0, \sigma^1, \dots, \sigma^{r-1}$  are the automorphisms of  $\text{GR}(4,r)$ . Then power polynomial substitution ( $\Psi_2$ ) over  $\text{GR}(4,r)$  is defined as follows.

$$\Psi_2^b(a) = 2^i(a_u^{\text{power } b_i}); \text{ where } a = 2^i a_u \quad (5.1.4)$$

where  $1 \leq b < 2^r - 1$ ,  $(b, 2^r - 1) = 1$  and  $(b, 2) = 1$ .

*Remark 5.1.1:* Observe that both the extensions of permutations defined over  $\text{GR}(4,r)$  collapse to permutation monomials for  $\text{GR}(2,r) = \text{GF}(2^r)$ .

**Lemma 5.1.2:** Let  $B(x)$  be a polynomial associated with any integer  $b$ ,  $0 < b \leq 2^r - 1$  given by

$$B(x) = b_0 + b_1 x + \dots + b_{r-1} x^{r-1}$$

where  $b_0, b_1, \dots, b_{r-1}$  are bits corresponding to binary representation of  $b$ , i.e  $B(2) = b$ . Then a power substitution  $x \longrightarrow x^{\text{power}(b)}$ , is a permutation on  $\text{GR}^*(4,r)$  if and only if

$$(b, 2^r - 1) = 1 \quad (5.1.5)$$

$$(B(x), x^r - 1) = 1 \quad (5.1.6)$$

**Proof:** One can easily verify that the above mapping is an automorphism on  $G_c \in \text{GR}^*(4,r)$ . We show that the mapping is also an automorphism on  $G_a \in \text{GR}^*(4,r)$ . Then because of the direct product structure of  $\text{GR}^*(4,r)$ , result follows. We know that elements of  $G_a$  are of order 2 and can be represented as  $a = 1 + 2a_1$ , where  $a_1 \in \{G_c \cup 0\}$ ,  $\cup$  represents Set theoretic union. Let  $b_{i_1}, b_{i_2}, \dots, b_{i_\gamma}$  be non-zero positions in the binary representation of  $b$ , then  $\Psi_2(a)$  becomes

$$\begin{aligned} \Psi_2(a) &= (\sigma^{i_1}(a) \sigma^{i_2}(a) \dots \sigma^{i_\gamma}(a)) \\ &= (1 + 2(\sigma^{i_1}(a_1) + \sigma^{i_2}(a_1) + \dots + \sigma^{i_\gamma}(a_1))) \\ &= (1 + 2(a_1^{2^{i_1}} + a_1^{2^{i_2}} + \dots + a_1^{2^{i_\gamma}})) \end{aligned}$$

This can be expressed in polynomial form as  $\Psi_2(a) = (1 + 2(B'(a_1)))$ , where  $B'(x)$  is a linearized polynomial over  $\{G_c \cup 0\}$  given by  $B'(x) = b_0 x + b_1 x^2 + \dots + b_{r-1} x^{2^{r-1}}$ . Since  $2\{G_c \cup 0\}$  is isomorphic to  $\text{GF}(2^r)$ , this implies that  $\Psi_2$  is an automorphism on  $G_a$  if and only if  $B'(x)$  is a permutation polynomial over  $\text{GF}(2^r)$ . From Chapter 7 of [67], the linearized polynomial  $B'(x)$  is a permutation polynomial if and only a  $r$  by  $r$  matrix  $A$  given by  $A_{ij} = (b_{i-j})^{2^j}$ ,  $0 \leq i, j < r$ , is nonsingular. Since  $b_i$  belongs to  $\text{GF}(2)$ ,  $(b_i)^{2^j}$  also belongs to  $\text{GF}(2)$ . Hence in this case  $A$  is a circulant matrix. Then from Chapter 16 of [24],  $A$  is nonsingular if and only if  $B(x)$  is relatively prime to  $x^r - 1$ . Result then follows immediately.  $\square$ .

### 5.1.2 Permutations over $PGR(V^k, r)$

The ideal basis representation of  $PGR(V^k, r)$  is used to define permutations here. An element  $\alpha \in PGR(V^k, r)$  in ideal basis is expressed as  $\alpha = \alpha'_0 + w\alpha'_1 + \dots + w^{k-1}\alpha'_{k-1}$ , where  $\alpha'_i \in SPGR(V, r) = GF(V^r)$ .

Then permutation  $P$  is defined as follows. Let  $\hat{P}$  be a permutation over  $SPGR(V, r)$ , then  $P$  is defined as

$$P(\alpha) = \hat{P}(\alpha'_0) + w\hat{P}(\alpha'_1) + \dots + w^{k-1}\hat{P}(\alpha'_{k-1}); \quad (5.1.7)$$

where  $\alpha = \alpha'_0 + w\alpha'_1 + \dots + w^{k-1}\alpha'_{k-1}$ . In fact, various permutations can be defined by employing different substitutions for individual coordinates of  $PGR(V^k, r)$  elements. For simplicity single permutation has been used for substitutions in all the coordinates. If  $\hat{P}$  is a permutation polynomial over  $SPGR(V, r)$ , then  $P$  is called permutation polynomial over  $PGR(V^k, r)$ .

**Permutation Monomial over  $PGR(V^k, r)$ :** Here the monomial substitution ( $\Psi$ ) is defined as follows. For any  $\alpha = \alpha'_0 + w\alpha'_1 + \dots + w^{k-1}\alpha'_{k-1} \in PGR(V^k, r)$ ,  $\alpha'_i \in SPGR(V, r)$

$$\Psi^b(\alpha) = (\alpha'_0)^b + w(\alpha'_1)^b + \dots + w^{k-1}(\alpha'_{k-1})^b, \quad (5.1.8)$$

where  $0 < b \leq V^r - 1$  and  $(b, V^r - 1) = 1$

**Lemma 5.1.3:** A generalized monomial  $\Psi^b$ ,  $x \longrightarrow \Psi^b(x)$ ,  $b$  an integer  $0 < b \leq (V^r - 1)$ , is a permutation polynomial on  $PGR(V^k, r)$  if and only if

$$(b, V^r - 1) = 1$$

**Proof:** Result follows from the definition of the polynomial substitution and the structure of  $SPGR(V, r)$ , whose group of units is cyclic group of order  $V^r - 1$ .  $\square$

**Remark 5.1.2:** Observe that the extensions defined over  $PGR(V^k, r)$  collapse to permutation monomials for  $PGR(V, r) = GF(V^r)$ .

## 5.2 General Procedure for Obtaining Sequences with Large Linear Complexity

### 5.2.1 Procedure for Sequences over Finite Field

One of the ways of generating sequences over finite field with large LC is as follows.

- 1: Consider a maximal length sequence  $\{y_i\}$  over the extension field  $GF(p^r)$
- 2: Each symbol  $y$  of  $\{y_i\}$  is mapped onto  $g(y)$  using permutation polynomial  $g(x)$  over  $GF(p^r)$ .
- 3: The sequence  $\{s_i\}$  is then defined as the trace function of  $\{y_i\}$ :  $s_i = \text{tr}_1^r(y_i)$
- 4: The resulting sequence  $\{s_i\}$  over  $GF(p)$  has large LC.

Support for obtaining sequences with large LC for the above mentioned steps is given as follows.

**Definition 5.2.1:** Polynomial sequence: Let  $f(x)$  denote a polynomial over  $GF(q)$ :

$$f(x) = \sum_{i=0}^{q-1} a_i x^i \quad (5.2.1)$$

If the symbol  $s_i$  of the sequence  $\{s_i\}$  are obtained as  $s_i = f(y_i)$ , where  $\{y_i\}$  is a sequence over  $GF(q)$ , then  $\{s_i\}$  is called polynomial sequence.

Following theorem due to Brynielsson [83] gives LC of polynomial sequences over  $GF(2^r)$ . Similar result exists for polynomial sequences over  $GF(p^r)$  [83].

**Theorem 5.2.1:** (Brynielsson [83]). Let  $\{y_i\}$  be an  $m$ -sequence over  $GF(2^r)$  with Linear span  $u$ . The polynomial sequence  $\{s_i\}$  with  $s_i = f(y_i)$  has linear complexity:

$$LC(\{s_i\}) = \sum_{a_i \neq 0} u^{H(i)}, \quad (5.2.1)$$

where  $H(i)$  is the number of ones present in the binary representation of  $i$ .

It is desirable that the polynomial sequence  $\{s_i\}$  over  $GF(2^r)$  {in general  $GF(p)$ } should preserve the correlation properties of the original sequence  $\{y_i\}$ . Hence the polynomial function  $f(x)$  which maps an element from  $GF(2^r)$  to  $GF(2)$  should have following properties

- (1)  $f$  is a mapping from  $GF(2^r)$  to  $GF(2)$  ( produces a binary sequence).
- (2)  $f$  is such that  $|\{x: f(x) = 1\}| = |\{x: f(x) = 0\}| = 0$ , where  $|\{.\}|$  represents the cardinality of the enclosing set  $\{.\}$ .
- (3)  $f$  produces a sequence of large linear complexity.
- (4)  $f$  is easy to implement.

Trace functions satisfy the above requirements, but it is a linear function. To obtain non-linear function, trace function is modified as follows. The conditions (1) and (2) are simultaneously satisfied by a function

$$f(x) = \text{tr}_1^r(g(x)), \quad x \in GF(2^r). \quad (5.2.3)$$

where  $g(x)$  permutes the finite field  $GF(2^r)$ . The amount of complexity enhancement depends on the permutation polynomial  $g(x)$  chosen for the sequence generation.

**Complexity Enhancement using Permutation Monomials:** Monomial  $x^b$  is a permutation polynomial of  $GF(q)$  if and only if  $b$  and  $q-1$  are relatively prime [Lidl]. Consider the function  $f(x) = \text{tr}_1^r(x^b)$ , where  $\text{gcd}(b, 2^r-1) = 1$ . By the definition of trace function,  $f(x)$  can be written as



$$f(x) = x^b + x^{b^2} + x^{b^2^2} + \dots + x^{b^{2^{r-1}}} \quad (5.2.4)$$

Then, from Theorem 5.2.1 the LC of the polynomial sequence  $\{s_i\}$  with  $s_i = f((x_i)^b)$  is given by

$$LC(\{s_i\}) = \sum_{a_i \neq 0} u^{H(i)}. \quad (5.2.5)$$

Observe that non-zero  $a_i$ 's occur only for indices  $i = b, 2b, 2^2b, \dots, 2^{r-1}b$ . Since all these indices are simply obtained by shifting binary representation of integer  $b$ ,  $H(i) = H(b)$  for  $i = b, 2b, 2^2b, \dots, 2^{r-1}b$ . The LC of  $\{s_i\}$  is given by  $u^{H(b)}r$ , where  $u$  is the LC of the sequence  $\{x_i\}$ .

**GMW Sequences:** If the monomial polynomial function is used in the complexity enhancement scheme, resultant sequence is a GMW sequence. Here  $\{x_i\}$  is a  $m$ -sequence over  $GF(2^r)$  of complexity  $u$ .

Then the GMW sequence  $\{s_i\}$  obtained from  $\{x_i\}$  is given by

$$s_i = \text{tr}_1^r(x^b), 0 < b < 2^r - 1, (b, 2^r - 1) = 1.$$

The linear complexity of the sequence is given by

$$LC(\{s_i\}) = u^{H(b)}r. \quad (5.2.6)$$

where  $H(b)$  is the number of ones present in the binary representation of  $b$ . If the trace function representation is followed, GMW sequence  $\{s_i\}$  is given by the following expression.

$$s_i = \text{tr}_1^r([\text{tr}_r^{ru}(a\alpha^i)]^b), i \in Z_{2^{ru}-1}. \quad (5.2.7)$$

## 5.2.2 Extension to Local Residue Class Rings $Z_4$ and $P_p^n[w^k]$

Here a complexity enhancement procedure is proposed for obtaining large LC sequences over local rings  $Z_4$  and  $P_p^n[w^k]$  on the lines of the procedure given in Section 5.2.1 for field sequences. Let  $\mathcal{R}$  denote the ring  $Z_4$  or  $P_p^n[w^k]$  and  $GR(\mathcal{R}, r)$  be the  $r^{\text{th}}$  degree Galois extension of  $\mathcal{R}$  ( $GR(4, r)$  or  $PGR(V^k, r)$ ). Steps for complexity enhancement of sequences over  $\mathcal{R}$  are given as follows:

- 1: Consider an  $m$ -sequence  $\{y_i\}$  over extension ring  $GR(\mathcal{R}, r)$  of LC  $u$ ,  $u$  being a positive integer.
- 2: Using a suitable permutation  $P$  on  $GR(\mathcal{R}, r)$ ,  $y_i$ 's are permuted;  $y_i' = P(y_i)$ ,  $y_i \in \{y_i\}$ .
- 3: The sequence  $\{s_i\}$  is then defined as the trace of  $\{y_i'\}$ ;
$$s_i = \text{tr}_1^r(y_i').$$
- 4: The resulting sequence  $\{s_i\}$  over  $\mathcal{R}$  has large LC.

In Section 5.3 we make use of permutations defined in Section 5.1 in the above procedure for

construction of sequences with large LC. It is desirable that the permutations employed in the procedure should preserve the correlation transform properties of resultant sequences. In this direction we give the definition for correlation preserving permutation.

**Definition 5.2.1:** A permutation is called as correlation preserving permutation if when it is used in the complexity enhancement procedure results in sequences which has same correlation transform as as those of  $m$ -sequences. For sequences over  $Z_4$  we have the following theorem

**Theorem 5.2.1:** If in the step 2 of the complexity enhancement procedure, permutation  $P = [P_1, P_2, P_3]$  on  $GR(4, r)$  is used, such that

$$P_1(\beta) = \sigma^i(\beta), \text{ for all } \beta \in G_a, \text{ where } \sigma^i, i=0, 1, \dots, r-1 \text{ are automorphisms of } GR(4, r),$$

$$P_2(.) \text{ and } P_3(.) \text{ are arbitrary permutations on } G_c,$$

then resulting sequences have same  $\aleph$ 's as those of  $m$ -sequences.

**Proof:** It is sufficient to prove the above theorem for permutation  $P' = [P'_1, P_2, P_3]$  with  $P'_1(\beta) = \beta$ , for all  $\beta \in G_a$  (identity permutation), since rest of the permutations  $P_1$  indicated in the theorem can be obtained by the permutations  $P_1 = \sigma^i(P'_1)$ ,  $0 \leq i < r$ , and sequences generated by the later will have the same  $\aleph$ 's as obtained with  $P'$  since  $\text{tr}(\sigma^i(\alpha)) = \text{tr}(\alpha)$ , for all  $i$ . A typical sequence  $S^a$  generated by a complexity enhancement procedure is given by

$$s_i = \text{tr}_1^r(P'[\text{tr}_r^{ru}(a\alpha^i)]), i \in Z_{2^{ru}-1}$$

where  $\alpha$  is primitive in  $GR(4, ru)$  and  $a \in G_a$  of  $GR^*(4, ru)$  and  $P'$  is a permutation of the type considered

in the theorem. let  $T = \frac{(2^{ru}-1)}{(2^r-1)}$ , then  $\alpha^T$  is primitive in  $GR(4, r)$ . The intermediate sequence  $\{s'_i\}$  is given by  $s'_i = \text{tr}_r^{ru}(a\alpha^{m^*T+k}) = \alpha^{m^*T} \{\text{tr}_r^{ru}(a\alpha^k)\}$ ,  $0 \leq m < 2^r-1$ ,  $0 \leq k < T$ ,  $i = m^*T+k$ . Hence  $s'_i$ 's belong to the set  $\{b_1(G_c), b_2(G_c), \dots, b_T(G_c)\}$ , where  $b_i$ 's are either 2 or elements belonging to  $G_a$ . Since the permutation  $P'$  simply permutes  $G_c$  and leaves  $G_a$  unaltered,  $\{s_i\}$  is some permuted version of an  $m$ -sequence  $\text{tr}_1^{ru}(a\alpha^i)$ . Hence  $\aleph$  of sequences are same as those of  $m$ -sequences.  $\square$

From (3.1.1), any element  $a \in G_a$  of  $GR(4, r)$  can be expressed as  $a = (1+2a')$ , where  $a' \in \{G_c \cup 0\}$ . In fact  $G_a = 1 + \langle 2 GR(4, r) \rangle$ . Also  $\langle 2 GR(4, r) \rangle$  is isomorphic to  $GF(2^r)$ . So permutation of  $G_a$  is essentially a permutation of finite field  $GF(2^r)$ .

According to Theorem 5.2.1, permutations  $P_1$  on  $G_a$  which preserves the correlations are of the type  $P_1(\beta) = \sigma^i(\beta)$ . Question is, are there more correlation preserving permutations. We conjecture that if

$P_1$  is such that  $P_1(\beta) = P_1(1 + 2\beta^r) = 1 + 2L(\beta^r)$ , where  $L(\cdot)$  is a linear permutation and  $\beta^r \in \{G_c \cup 0\}$ , then resultant sequences have  $m$ -sequence type correlation transforms. Note that the automorphism permutations considered in Theorem 5.2.1 is a special case of linear permutation.

We state our conjecture as follows.

*Conjecture 5.2.1:* If in the step 2 of the complexity enhancement procedure, permutation  $P = [P_1, P_2, P_3]$  on  $GR(4, r)$  is used, resultant sequences have  $\aleph$  same as those of  $m$ -sequences of period  $2^{ru}-1$  if and only if  $P$  is of the following type.

$$P_1(\beta) = P_1(1+2\beta^r) = (1 + 2 L(\beta^r)), \text{ for all } \beta \in G_a,$$

where  $L(\cdot)$  denotes a linear permutation and  $\beta^r \in \{G_c \cup 0\}$ ;

and  $P_2(\cdot)$  and  $P_3(\cdot)$  are arbitrary permutations on  $G_c$ .

Thus correlation transform values of sequences generated using correlation preserving permutations in complexity enhancement procedure given in Section 5.2.2 belongs to the  $\aleph$  values of  $m$ -sequences of period  $2^{ru}-1$ ;  $\aleph$  values belongs to the set

$$\begin{aligned} &\{-1, \pm 2^t-1 \pm \omega 2^t\} \text{ whenever } ru \text{ is odd, } ru = 2t+1 \\ &\{-1, \pm 2^t-1, -1 \pm \omega 2^t\} \text{ whenever } ru \text{ is even, } ru = 2t, \text{ where } \omega = \sqrt{-1}. \end{aligned}$$

### 5.3 Generalized GMW (GGMW) Sequences over $Z_4$ and $P_p^n[w^k]$

Associated with a  $\mathcal{A}$  family over  $Z_4$  (or  $P_p^n[w^k]$ ) a family of GGMW sequences over  $Z_4$  (or  $P_p^n[w^k]$ ) is defined; the GGMW sequences formed by transforming the  $m$ -sequences using a permutation monomial in the complexity enhancement procedure given Section 5.2. The family includes a GMW sequence over residue field also.

#### 5.3.1 GGMW Sequences over $Z_4$

Family of GGMW sequences over  $Z_4$  is a collection of  $2^{ru}+1$  sequences each of period  $2^{ru}-1$ . The family includes a GMW sequence over an ideal  $\langle 2 \rangle \cong GF(2)$  also. Corresponding to an element  $A$ , a GGMW sequence  $S^A = \{s_i\}$  is given by

$$s_i = \text{tr}_1^r(\Psi[\text{tr}_r^{ru}(A\alpha^i)]), i \in Z_{2^{ru}-1}. \quad (5.3.1)$$

where  $\Psi(\cdot)$  is a generalized permutation monomial. There are  $2^{ru}$  distinct zero level sequences given by a set  $\{S^A, A \in G_a\}$ . The only first level sequence (isomorphic to GMW sequence over  $GF(2)$ ) is  $S^2$ . We have

two types of families of GGMW sequences corresponding to two types of permutation monomials ( $\Psi_1$  and  $\Psi_2$ ) defined in Section 5.2. They are denoted as  $\text{GGMW}^{\Psi_1}$  and  $\text{GGMW}^{\Psi_2}$ .

Fig 5.3.1 gives schematic diagram of generation of quadriphase sequences derived from GGMW sequences over  $Z_4$ .

**Number of Distinct Family of GGMW Sequences over  $Z_4$ :** Next theorem gives different possible family of GMW sequences and allowable choices for the permutations for the intermediate ring.

**Definition: 5.3.1: Equivalent Permutations:** Two permutations  $\Psi^1$  and  $\Psi^2$  are equivalent permutations on  $\text{GR}(4,r)$  if  $\Psi^2$  can be obtained as some automorphism of  $\Psi^1$  i.e.

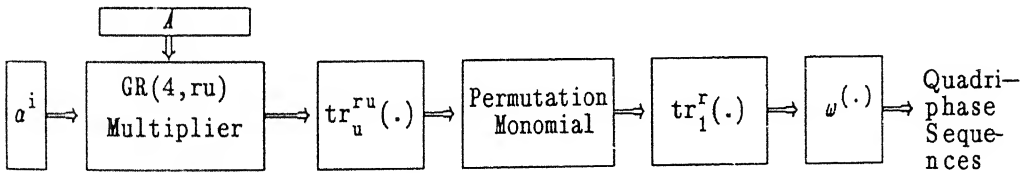
$$\Psi^1 = \sigma^i(\Psi^2), \text{ where } \sigma^i, i = 0, 1, \dots, r-1, \text{ automorphisms of ring } \text{GR}(4,r).$$

**Theorem 5.3.1:** Let  $F_1$  and  $F_2$  be two families of GGMW sequences as defined in (5.3.1) which uses  $\Psi$  and  $\Psi'$  permutation monomials respectively and has  $\alpha$  and  $\alpha^d$  respectively as element belonging to  $G_a$  for sequence generation. Then two families are cyclically equivalent if and only if

$$d = 2^m \text{ for some } 0 \leq m < ru$$

and  $\Psi^1, \Psi^2$  are equivalent permutations on  $\text{GR}(4,r)$   $\Psi^1 = \sigma^i(\Psi^2)$ , for some  $i$ .

**Proof:** The above conditions are necessary since, if two families are cyclically equivalent, their zeroth level sequences (GMW sequences over  $\text{GF}(2)$ ) also have to be cyclically equivalent; two cyclically equivalent



$$A \in \text{GR}(4,ru), r \text{ and } u \text{ are positive integers}$$

$$\alpha \text{ is primitive in } G_c \text{ of } \text{GR}(4,r)$$

$$\omega = \sqrt{-1}$$

**Fig 5.3.1 Schematic Diagram of Generation of Quadriphase Sequences**

**Derived from GGMW Sequences**

binary GMW sequences satisfy the required condition (Theorem 4 of [48]). Sufficiency can be easily seen because of the trace property A9 (Appendix A).  $\square$

In view of the Theorem 5.3.1 and because of the fact that the element  $\alpha$  used to generate the sequences is primitive, the number of distinct families are given by

$$N_{\text{GMW}} = (\phi(2^r - 1) / ru) N(r) \quad (5.3.2)$$

where  $\phi$  is Euler's  $\phi$  function and  $N(r)$  is equal to number of distinct non-equivalent permutations on  $\text{GR}(4, r)$ .

**Lemma 5.3.1:** The number of distinct non-equivalent permutation monomials of the first type ( $\Psi_1$ ) is given by

$$N^{\Psi_1}(r) = \phi(2^r - 1) \text{ where } \phi \text{ is Euler's } \phi \text{ function.}$$

**Proof:** From Lemma 5.1.1 there are  $\phi(2^r - 1)$  different permutations for every  $r$ . The permutation  $\Psi_1$  only permutes  $G_c$  and leaves  $G_a$  unchanged; ie. if  $a\alpha \in \text{GR}(4, r)$  where  $a \in G_a$  and  $\alpha \in G_c$ , then  $\Psi_1(a\alpha) = a\alpha^b$ . For any nonzero  $i$ ,  $i^{\text{th}}$  automorphism of  $\Psi(a\alpha)$ ,  $\sigma^i(\Psi)(a\alpha)$ , is given by  $\sigma^i(a)\alpha^{b^i}$ ,  $b^i = b2^i$ . Thus  $\sigma^i(\Psi)(a\alpha)$  cannot be written as  $\Psi'_1$  permutation of  $a\alpha$  where  $\Psi'_1$  is another permutation monomial of the first type. Hence all  $\Psi_1$ 's are distinct.  $\square$

**Lemma 5.3.2:** The number of distinct non-equivalent permutation monomials of the second type ( $\Psi_2$ ) is given by  $\phi'(r)/r$ , where  $\phi'(r) = |\{B(x), \deg(B(x)) < r, (B(2), 2^r - 1) = 1 \text{ and } (B(x), x^r - 1) = 1\}|$ ;

**Proof:** If  $B(x)$ , a polynomial of degree  $< r$  satisfies conditions mentioned in the Lemma, monomial  $\Psi_2^b$ ,  $b = B(2)$  is a permutation from Lemma 5.1.2. Moreover, if  $B(x)$  satisfies the above conditions, polynomial  $xB(x) \bmod x^r - 1$  also satisfies the above conditions. Let  $\Psi_2, \Psi'_2$  be the permutations corresponding to polynomial  $B(x)$  and  $xB(x)$  respectively. Then from the definition of the permutation it is easily seen that  $\Psi'_2 = \sigma(\Psi_2)$ . Hence permutations corresponding to  $B(x)$  and  $xB(x)$  are equivalent. There are  $r$  such permutations corresponding to polynomials  $(x^i B(x)) \bmod x^r - 1$ ,  $0 \leq i < r$ , which are equivalent. Thus there are exactly  $\phi'(r)/r$  permutation polynomials.  $\square$

Using Theorem 5.3.1 and above two lemmas, the number of cyclically distinct families of GGMW sequences with permutation monomials  $\Psi_1$  and  $\Psi_2$  is given by

$$N_{\text{GGMW}}(\Psi_1) = (\phi(2^r - 1) / ru) \phi(2^r - 1) \quad (5.3.3)$$

$$N_{\text{GGMW}}(\Psi_2) = (\phi(2^r - 1) / ru)(\phi'(2^r - 1)/r) \quad (5.3.4)$$

where  $\phi$  and  $\phi'$  are functions as defined in Lemma 5.3.1 and Lemma 5.3.2

### 5.3.2 GGMW Sequences over $P_p^n[w^k]$

Generalized GMW sequences over  $P_p^n[w^k]$  is a collection of  $V^{(k-1)ru} + V^{(k-2)ru} + \dots + V^{ru} + 1$  sequences each of period  $V^{ru}-1$ . This class includes a GMW sequence over  $\langle w^{k-1} \rangle$  which is isomorphic to  $GF(V)$ . Corresponding to an element  $A$ ,  $A \in PGR(V^k, r)$ , GGMW sequence  $S^A = \{s_i\}$  is given by

$$s_i = \text{tr}_1^r(\Psi^b[\text{tr}_r^{ru}((A\alpha^i))]), i \in Z_{2ru-1} \quad (5.3.5)$$

where  $\Psi^b(\cdot)$  is a generalized permutation monomial over  $PGR(V^k, r)$  defined in Section 5.1.

As in the case of  $\mathcal{A}$  families, we have  $k$  distinct level sequence groups.  $\kappa^{\text{th}}$  level sequences over  $P_p^n[w^k]$  are isomorphic to zeroth level sequences of over ring  $P_p^n[w^{k-\kappa}]$ . Thus it is sufficient to consider only zeroth level sequences. There are  $V^{(k-1)ru}$  distinct zeroth level sequences given by the set  $\{S^A, A \in G_a\}$ , where  $G_a$  is the Abelian component group of group of units  $PGR^*(V^k, ru)$ .  $k-1^{\text{th}}$  level sequence (isomorphic to GMW sequence over  $GF(V)$ ) is  $S^{w^{k-1}}$ .

### 5.3.3 Generalized $r$ -tuple Distributions

**Definition 5.3.2:** A family  $F$  of  $(V^{r(k-1)} + V^{r(k-2)} + \dots + V^r + 1)$  sequences over a ring of size  $V^k$ , each of period  $V^r-1$ , where  $V$ ,  $k$  and  $r$  are positive integers, exhibits an ideal  $\rho$ -tuple distribution  $Y$ ,  $0 \leq \rho \leq r$ , if exactly one of the  $V^{\rho k}$  possible and disjoint ring  $\rho$ -tuples occurs  $(V^{k(r-\rho)} - 1)$  times in one period of all sequences in  $F$  and each of the others occurs  $(V^{k(r-\rho)} - 1)$  times.

In case of finite fields, the definition of  $r$ -tuple distribution applies only to a single sequence. This may be from the consideration of length and order of finite field sequences; sequences of length  $V^r-1$  over a finite field of size  $V$  exists. The concept here has been extended to a family of sequences. Occurrences of tuples are now counted in a period of all sequences in the family.

**Lemma 5.3.3:** An ideal  $\rho$ -tuple distribution of  $Y$  implies ideal  $\rho'$  tuple distribution of  $Y$  for all  $\rho'$  with  $0 \leq \rho' \leq \rho$ .

**Proof:** From an ideal  $\rho$  tuple distribution, exactly one of the possible  $V^{\rho k}$  ring  $\rho$ -tuples occurs  $V^{k(r-\rho)} - 1$  times and each of the other occurs  $V^{k(r-\rho)}$  times. Therefore, exactly one  $\rho'$ -tuple occurs  $(V^{k(r-\rho)} - 1) + V^{k(r-\rho)} (V^{k(\rho-\rho')} - 1) = V^{k(r-\rho')} - 1$  and each of the other occurs  $V^{k(r-\rho)} V^{k(\rho-\rho')} = V^{k(r-\rho')}$  times. Hence the result.  $\square$

**Theorem 5.3.2:** Let  $\mathcal{R}$  be either a ring  $Z_{p^k}$  or  $P_p^n[w^k]$  of order  $V^k$ , with residue field  $GF(V)$  and  $GR(\mathcal{R}, r)$  be the  $r^{\text{th}}$  degree Galois extension ring of  $\mathcal{R}$ . Let  $F$  be a family of  $(V^{rm(k-1)} + V^{rm(k-2)} + \dots + V^{rm+1})$   $m$ -sequences over  $GR(\mathcal{R}, r)$  of LC  $m$  and period  $V^{rm}-1$ , then the transformed family of sequences  $F'$  by a generalized permutation  $P$  over  $\mathcal{R}$  exhibits  $\rho$ -tuple distribution for all  $\rho$  with  $0 \leq \rho \leq m$ , if and only if,

$$|\{x: P(x) = a, x \in GR(\mathcal{R}, r)\}| = V^{k(r-1)}, \text{ for all } a \in \mathcal{R} \quad (5.3.6)$$

where  $|\{.\}|$  denotes the cardinality of the enclosed set  $\{.\}$ .

**Proof:** All  $m$ -tuples  $\underline{x}_i = \{x_i, x_{i+1}, \dots, x_{i+r-1}\}$  in sequences in  $F$  are disjoint and every possible  $V^k$ -ary non-zero  $m$ -tuple occurs exactly once. The  $m$ -tuples in sequences over  $\mathcal{R}$  of  $F'$  occur from  $\underline{x}_i = \{x_i, x_{i+1}, \dots, x_{i+r-1}\}$  as  $\underline{y}_i = \{y_i, y_{i+1}, \dots, y_{i+r-1}\}$  with  $y_i = P(x_i)$ . It is easy to see that (5.3.6) is necessary since 1-tuple distribution implies (5.3.6). The sufficiency of (5.3.6) is shown as follows. Let  $P(0) = 0$ . From (5.3.6), there are  $V^{k(r-1)}$  elements in  $GR(\mathcal{R}, r)$  whose image in  $\mathcal{R}$  is 0. Thus  $V^{k(r-1)m-1}$  ( $=V^{k(rm-m)}-1$ )  $m$ -tuples  $\underline{x}_i$  are mapped to  $\underline{y}_i = 0$  where  $-1$  accounts for missing 0  $m$ -tuple in sequences of  $F$ . Similarly there are  $V^{k(rm-m)}$   $m$ -tuples in  $F$  which maps into a unique non-zero  $m$ -tuple in  $F'$ . The arguments can be repeated if  $P(0)=a$ . Result then follows from Lemma 5.3.3.  $\square$

By using Theorem 5.3.2, it can be easily verified that families of GGMW sequences satisfy ideal generalized  $r$ -tuple distribution stated above.

## 5.4 Properties of Families of GGMW Sequences over $Z_4$

From the definitions of permutation monomials given Section 5.2, it is easy to verify that permutation monomials of first and second type ( $\Psi_1$  and  $\Psi_2$ ) over  $GR(4, r)$  are correlation preserving permutations. Hence correlation transform ( $\aleph$ ) values of GGMW sequences of period  $2^{ru}-1$  over  $Z_4$  takes on same values as those family of  $m$ -sequences of period  $2^{ru}-1$ . Thus correlation transform distributions of families of GGMW sequences are same as those given for  $m$ -sequence families (Ref Table 3.4.2). However, crosscorrelation distributions differ from those of  $m$ -sequence families. This is because in general GGMW sequences are nonlinear in nature (sequences are not closed under point wise addition) whereas  $m$ -sequence families are linear. Crosscorrelation distribution of a family of sequences depends on  $\aleph$  of difference (point wise subtraction) of various time shifted versions of sequences and if the family is linear computation of crosscorrelation distribution is related to correlation transform distribution. Thus, in this case determination of crosscorrelation properties is not straight forward. We have made some computer simulations for checking the crosscorrelation values of some GGMW families. The computer analysis

reveals that  $\theta_{\max}$  deviates from optimal value of  $\sqrt{L}$ ,  $L$  is the period of sequences. But it is observed that  $\theta_{\text{avg}}$  (averaged over all sequences and its time shifts) and  $\theta_{\text{rms}}$  (root mean square of crosscorrelation values over all sequences and its time shifts) are approximately equal to  $\sqrt{L}$ . Definitions of  $\theta_{\text{avg}}$  and  $\theta_{\text{rms}}$  are given in (2.5.2) and (2.5.3). In Section 5.4.1, we prove that  $\theta_{\text{rms}}$  for GGMW families is approximately equal to  $\sqrt{L}$  by showing that families of GGMW sequences satisfy Welch bound with equality (refer Section 2.5). Section 5.4.2 gives some computer results concerning autocorrelation and crosscorrelation values of families of GGMW sequences. A generalized autocorrelation function is defined in Section 5.4.3 and it is shown that out of phase generalized autocorrelation values of GGMW sequences are uniformly  $-1$ .

### 5.4.1 GGMW Families Satisfying Welch bound with Equality

Consider a GGMW sequence family of period  $2^{\text{ru}}-1$ , and let  $G$  be a set of zeroth level sequences given by  $G = \{S^A, A \in G_a \text{ of } \text{GR}^*(4, \text{ru})\}$

**Lemma 5.4.1:** An element  $\text{tr}_r^{\text{ru}}(A\alpha^i)$ ;  $A \in G_a$ ,  $\alpha \in G_c$  is a unit or a zero divisor if and only if  $\text{tr}_r^{\text{ru}}(\alpha^i)$  is a unit or a zerodivisor and thus  $\text{tr}_r^{\text{ru}}(A\alpha^i)$ ,  $\text{tr}_r^{\text{ru}}(B\alpha^i)$ ,  $A, B \in G_a$  are simultaneously both zero divisors or units.

**Proof:** Using P6 of Section 3.1,  $\text{tr}_r^{\text{ru}}(A\alpha^i)$  and  $\text{tr}_r^{\text{ru}}(B\alpha^i)$ ,  $A, B \in G_a$ , can be written as

$$\begin{aligned}\text{tr}_r^{\text{ru}}(A\alpha^i) &= \text{tr}_r^{\text{ru}}(\alpha^i) + 2 \text{tr}_r^{\text{ru}}(A'\alpha^i), \\ \text{tr}_r^{\text{ru}}(B\alpha^i) &= \text{tr}_r^{\text{ru}}(\alpha^i) + 2 \text{tr}_r^{\text{ru}}(B'\alpha^i),\end{aligned}$$

where  $A', B' \in G_c$ . Then the homomorphic mapping  $(\mu)$  from  $Z_4$  to  $Z_2$  (taking modulo 2) on the above equations gives  $\mu(\text{tr}_r^{\text{ru}}(A\alpha^i)) = \mu(\text{tr}_r^{\text{ru}}(\alpha^i)) = \mu(\text{tr}_r^{\text{ru}}(B\alpha^i))$ , since  $\mu$  of any zerodivisor is always 0. Thus  $\text{tr}_r^{\text{ru}}(A\alpha^i)$  and  $\text{tr}_r^{\text{ru}}(B\alpha^i)$  are simultaneously units or zero divisors. Similarly first part of the theorem is also clear.  $\square$

Consider a set of vectors  $G^{\alpha^j}$ ,  $0 \leq j < 2^{\text{ru}}-1$ , containing  $j^{\text{th}}$  cyclic shifts of zeroth level GGMW sequences.

$$G^{\alpha^j} = \{S^A\alpha^j, \text{ for all } A \in G_a \text{ of } \text{GR}^*(4, \text{ru})\}$$

We have Lemma 5.4.2 on the sum of quadriphase inner-products of  $G^{\alpha^j}$ .



**Lemma 5.4.2:** The set of quadriphase vectors derived from  $G^{\alpha^j}$ ,  $0 \leq j < 2^{ru}-1$ , satisfies Welch bound with equality.

**Proof:** Consider any two sequences  $S^{A\alpha^j}$ ,  $S^{B\alpha^j} \in G^{\alpha^j}$  and consider their corresponding intermediate sequences  $\hat{S}^{Aj}$  and  $\hat{S}^{Bj}$ , over  $GR(4,r)$ ;  $m^{\text{th}}$  element of  $\hat{S}^{Aj}$  is given by  $s'_m = \text{tr}_r^{ru}(A\alpha^{j+m})$ . Then the inner-product correlation between  $S^{A\alpha^j}$ ,  $S^{B\alpha^j}$  is given by

$$C_{AB}(0) = \Re(S^{A\alpha^j} - S^{B\alpha^j}) = \frac{T-1}{\sum_{m=0}^{T-1}} \frac{2^r-2}{\sum_{n=0}^{2^r-2}} [\delta(m,n)]$$

where  $\delta(m,n) = (\text{tr}_1^r(\Psi(a_m \hat{\alpha}_m)) - (\text{tr}_1^r(\Psi(b_m \hat{\alpha}'_m)))$ ,  $T = \frac{(2^{ru}-1)}{(2^r-1)}$ ,  $\beta = \alpha^T \in G_c$  of  $GR(4,r)$ ;  $a_m \hat{\alpha}_m = \text{tr}_r^{ru}(A\alpha^{j+m})$ ,  $b_m \hat{\alpha}'_m = \text{tr}_r^{ru}(B\alpha^{j+m})$ ;  $\hat{\alpha}_m, \hat{\alpha}'_m$  takes either 2 or from  $G_c$  of  $GR(4,r)$ . From Lemma 5.4.1,  $\hat{\alpha}_m = \hat{\alpha}'_m$  and  $a_m \hat{\alpha}_m$  and  $b_m \hat{\alpha}'_m$  are simultaneously zero divisors or units. By substituting for  $\Psi_1$  or  $\Psi_2$  when  $a_m \hat{\alpha}_m$  and  $b_m \hat{\alpha}'_m$  are both units,  $\delta(m,n)$  becomes

$$\begin{aligned} \delta(m,n) &= \text{tr}_1^r((1+2L(a'_m))\hat{\alpha}_m^b \beta^{bm}) - \text{tr}_1^r((1+2L(b'_m))\hat{\alpha}_m^b \beta^{bm}) \\ &= \text{tr}_1^r((2L(a'_m - b'_m))\alpha_m^b \beta^{bm}) \in \langle 2 \rangle, \end{aligned}$$

where  $L(\cdot)$  is a linear function on  $G_a$ ; it is identity function when the monomial is  $\Psi_1$ , and a linearized polynomial function when the monomial is  $\Psi_2$ . When  $a_m \hat{\alpha}_m$  and  $b_m \hat{\alpha}'_m$  are both zero divisors,  $\delta(m,n)$  is given by  $\delta(m,n) = \text{tr}_1^r(2(a'_m - b'_m)\beta^{bm}) \in \langle 2 \rangle$ . Thus in any case,  $(S^{A\alpha^j} - S^{B\alpha^j})$  is some permutation of a sequence obtained when  $\Psi$  is identity, i.e. when  $S^{A\alpha^j}$  and  $S^{B\alpha^j}$  are both  $m$ -sequences over  $Z_4$ . Also from the above equations,  $(S^{A\alpha^j} - S^{B\alpha^j})$  is a sequence over  $\langle 2 \rangle$  and, hence is a permutation of an  $m$ -sequence over  $\langle 2 \rangle$ . Thus, we have

$$C_{AB}(0) = \Re(S^{A\alpha^j} - S^{B\alpha^j}) = \Re(m\text{-sequence over } \langle 2 \rangle) = -1.$$

Hence, the inner-product between any two vectors in  $G^{\alpha^j}$  is always  $-1$ . Let us compute the sum of all inner-products between the sequences in  $G^{\alpha^j}$  (Total energy, TE); it is given by

$$TE = \sum_{A \in G^{\alpha^j}} \sum_{B \in G^{\alpha^j}} |C_{AB}|^2,$$

From the above calculations,  $|C_{AB}|^2 = (2^{ru}-1)^2$  whenever  $A = B$  and  $|C_{AB}|^2 = 1$  whenever  $A \neq B$ .

Hence, TE is given by

$$TE = 2^{ru}(2^{ru}-1)^2 + 2^{ru}(2^{ru}-1)(1) = (2^{ru})^2 (2^{ru}-1)^2 / (2^{ru}-1) = \frac{(M \ E)^2}{L},$$

where  $M = 2^{ru}$ , the cardinality of the set  $G^{\alpha^j}$ . The result then follows from Theorem 2.5.1.  $\square$

**Theorem 5.4.1:** Families of GGMW sequences satisfy Welch bound with equality and hence mean square of the cross correlations,  $C_{rms}^2$  is approximately equal to the period,  $2^{ru}-1$ .

**Proof:** From Lemma 5.4.2, sets  $G^{\alpha^j}$ ,  $0 \leq j < 2^{ru}-1$  satisfy Welch bound with equality. Similarly it is easy to see that set of all cyclic shifts of  $\langle 2 \rangle$  ideal sequences along with a all zero sequence,  $G^2$ , also satisfies Welch bound with equality. Then from Lemma 2.5.1, the set which is the union of all sets  $G^{\alpha^j}$ ,  $0 \leq j < 2^{ru}-1$ , and  $G^2$  satisfies Welch bound with equality. This implies that family of GGMW sequences satisfies Welch bound with equality and the result then follows from Theorem 2.5.3.  $\square$

### 5.4.2 Autocorrelation and Crosscorrelation Properties of GGMW Sequences

In general GGMW family of sequences is a set of  $2^{ru}+1$  nonlinear sequences (sequences are not closed under point wise addition). Hence autocorrelation and crosscorrelation values are different from  $\Re$  of individual sequences. Let  $S^A = \{s_i\}$  be a GGMW sequence associated with  $A \in GR^*(4,r)$ ; it is given by  $s_i = \text{tr}_1^r(\Psi[\text{tr}_r^{ru}(A\alpha^i)])$ , where  $A = (1+2A') \in G_a$  of  $GR^*(4,ru)$ ,  $A' \in G_c$  of  $GR^*(4,ru)$ . Let  $\hat{S}^A = \{\hat{s}_i\}$  be the intermediate sequence over  $GR(4,r)$  of  $S^A$ ;  $\hat{s}_i = \text{tr}_r^{ru}((1+A')\alpha^i)$ . Thus  $\hat{S}^A = \hat{S}^1 + \hat{S}^{2A'}$ ,  $+$  : pointwise addition. Autocorrelation of the sequence  $S^A$ ,  $CA_A(\gamma)$ ,  $0 \leq \gamma < 2^{ru}-1$  given by

$$CA_A(\gamma) = \Re\{S^A + T^\gamma(S^A)\} \quad (5.4.1)$$

Similarly crosscorrelation function between  $S^A$  and  $S^B$ ,  $C_{AB}(\gamma)$ ,  $0 \leq \gamma < 2^{ru}-1$ , is given by

$$C_{AB}(\gamma) = \Re\{S^A + T^\gamma(S^B)\} \quad (5.4.2)$$

Thus the correlation functions of GGMW sequences in general depend on four intermediate sequences. But  $CA^1(\gamma)$  depends only on correlation transform of sum of  $S_1$  and  $\gamma^{\text{th}}$  cyclic shifted version of  $S^1$ . We call  $S^1$  a prime sequence in the family of GGMW sequences. A Complementary sequence  $S_3 = 3S_1$  is another prime sequence whose autocorrelation function depends only on two intermediate sequences. Also  $S^2 = 2S^1$  is a binary GMW sequence which has two level ideal autocorrelation function. Some computer simulations are conducted on correlation values of GGMW sequences. The computer analysis reveals that the magnitude of correlation values deviates from the optimal value of  $\sqrt{L}$  by a small value for majority of cases. However large deviations do occur but number such occurrences is very small. Also it is observed that  $\theta_{avg}$  is approximately equal to the optimum value of  $\sqrt{L}$ . Table 5.4.1 gives autocorrelation values along with  $\theta_{avg}$  values of some prime GGMW sequences.

Table 5.4.1 Autocorrelation Values of a Prime GGMW Sequence  $S^1$ 

r	u	period L	type of Monomial	$\theta_{\max}$	$\theta_{\text{avg}}$
3	2	63	$\Psi_1^3$	8.06	3.5
4	2	255	$\Psi_2^7$	26.02	12
3	3	512	$\Psi_1^3$	50.61	16

Results of computer analysis of some class of GGMW sequences are shown in the graphs given below. In Examples 5.4.1 and 5.4.2, we consider GGMW families of period 63 and 255 respectively.

*Example 5.4.1:* GGMW sequences of period 63,  $r = 3$ ,  $u = 2$ ; Intermediate ring in this case is  $GR(4,3)$ . Permutation monomial of the first type ( $\Psi_1^3$ ) is considered. Fig 5.4.1 gives autocorrelation distribution of selected GGMW sequences. Autocorrelation distribution curve of a prime sequence  $S^1$  is marked separately. Crosscorrelation distribution of the GGMW family is plotted in Fig 5.4.2.

*Example 5.4.2:* GGMW sequences of period 255,  $r = 4$ ,  $u = 4$ ; Intermediate ring is  $GR(4,4)$ . Monomial of the second type is used;  $\Psi_2 : x \mapsto x^{\text{power } 7}$ . Fig 5.4.3 gives autocorrelation distribution of some selected sequences. Distribution of crosscorrelation values between  $S^1$  and all other sequences in the family is given Fig 5.4.4.

### 5.4.3 Generalized Auto Correlation Properties of GGMW Sequences

Consider a set of  $M$  complex valued sequences, then generalized autocorrelation function  $GA(\tau)$  is defined as

$$GA(\tau) = \sum_{m=1}^M C_{mm}(\tau) \quad (5.4.3)$$

The set of  $2^{ru}+1$  GGMW Sequences have two level generalized autocorrelation function.  $GA(\tau)$  for a family of GGMW sequences can be written as

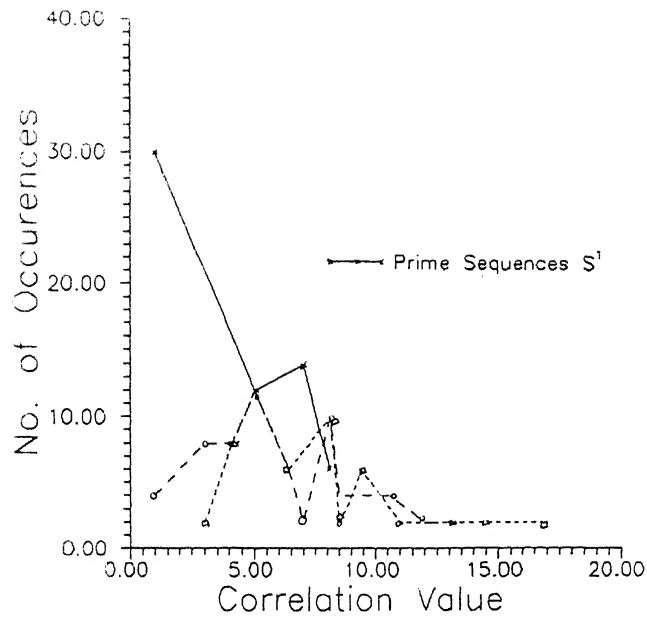


Fig 5.4.1 Autocorrelation Distribution of Selected GGMW sequences of Period 63  
(Example 5.4.1)

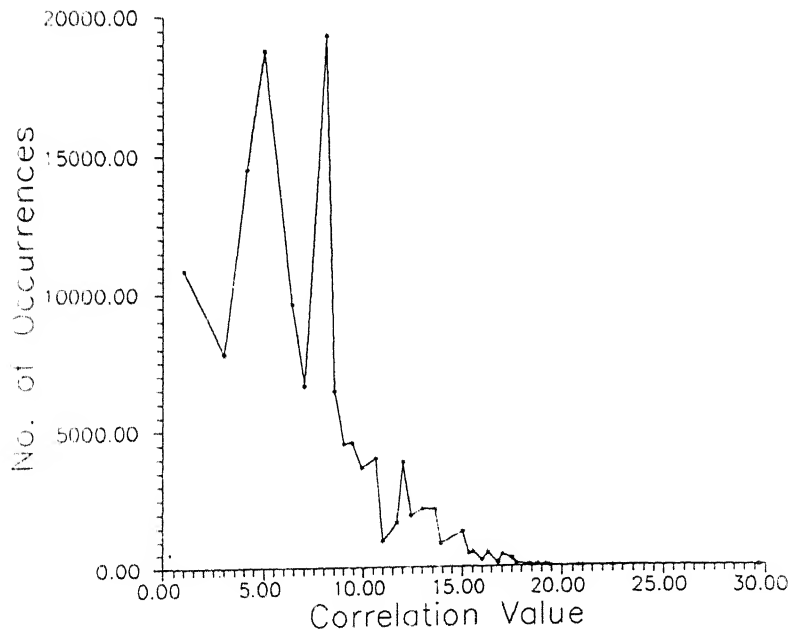


Fig 5.4.2 Crosscorrelation Distribution of GGMW sequences of Period 63

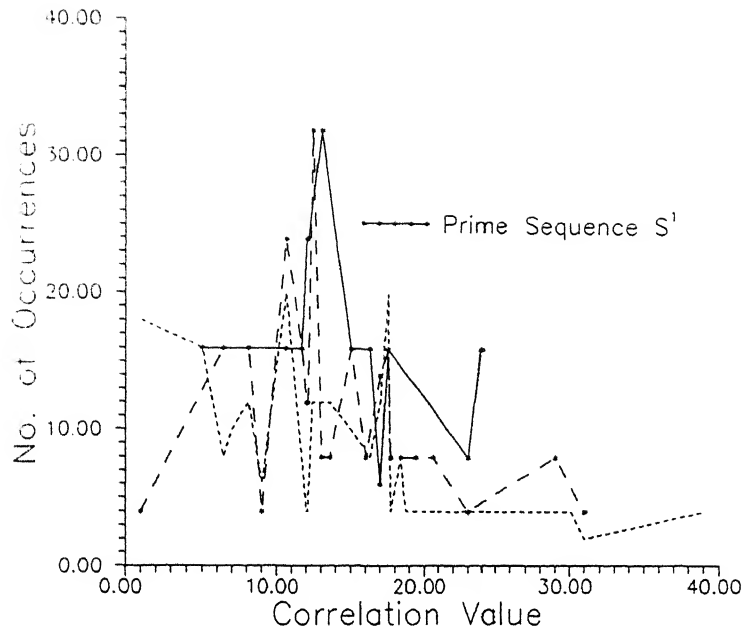


Fig 5.4.3 Autocorrelation Distribution of Selected GGMW sequences of Period 255  
(Example 5.4.2)

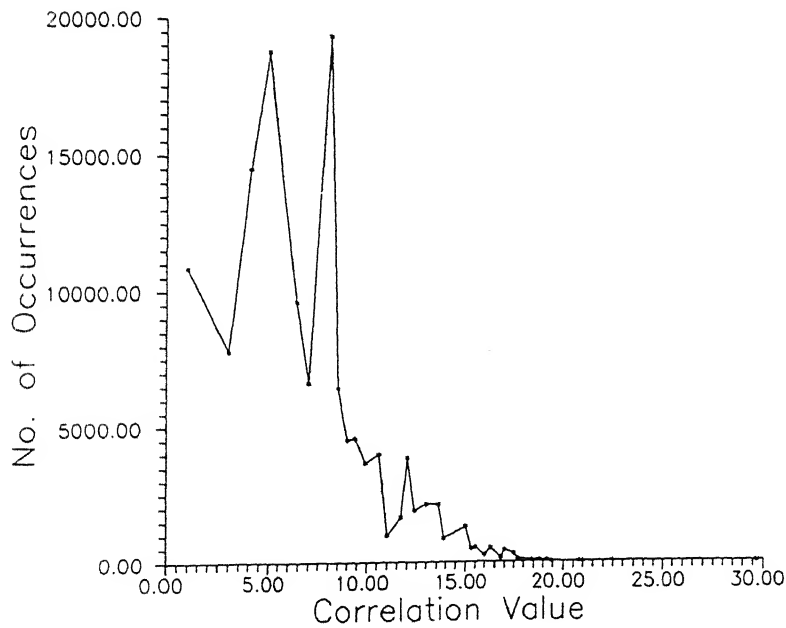


Fig 5.4.4 Distribution of Correlation Values between  
 $S^1$  and all GGMW sequences of Period 255 (Example 5.4.2)

$$GA(\tau) = \sum_{A \in \text{GGMW}} \Re(S^A - S^A \alpha^\tau).$$

When  $\tau = 0$ , obviously the value of  $GA(\tau)$  is  $4^{ru}-1$ . We shall show that  $GA(\tau)$  is  $-1$  whenever  $\tau \neq 0$ . This is a consequence of GGMW families satisfying Welch bound with equality. Consider a matrix of  $4^{ru}$  by  $2^{ru}-1$  entries,  $M^G$ , with first  $4^{ru}-1$  rows filled by quadriphase sequences obtained from all phases of GGMW sequences and last row filled by all one sequence.

$$M^G_{i,j} = \phi(S_j^A \alpha^n); 0 \leq m < 2^{ru}+1, 0 \leq n < 2^{ru}-1, i = (2^{ru}-1)m + n, 0 \leq j < 2^{ru}-1 \quad (5.4.4)$$

$$M^G_{4^{ru},j} = 1, 0 \leq j < 2^{ru}-1$$

where  $S_j^A, 0 \leq m < 2^{ru}+1$  are GGMW sequences of period  $2^{ru}-1$ . By using the fact that GGMW family satisfies Welch's bound with equality vectors in  $M^G$  can be shown to satisfy Welch bound with equality.

Then from Appendix E, inner-product between zeroth and  $\tau^{\text{th}}$  column in  $M_{\text{GGMW}}$  is zero. This implies

$$C^{0\tau} = \sum_{i=0}^{4^r} \phi(S_0^A \alpha^n) \phi(S_\tau^A \alpha^n)^* = 0$$

$$\sum_{i=0}^{2^{ru}+1} \sum_{n=0}^{2^{ru}-1} \phi(S_0^A \alpha^n) \phi(S_\tau^A \alpha^n)^* + 1 = 0.$$

The value  $+1$  in the LHS is due to the contribution of all one vector of  $M_G$ . From the definition of sequences  $S_0^A \alpha^n = S_n^A$ , and hence inner sum is equal to  $\Re(S^A - S^A \alpha^\tau)$ . Thus we have

$$\sum_{A \in \text{GGMW}} \Re(S^A - S^A \alpha^\tau) + 1 = 0.$$

Hence  $GA(\tau), \tau \neq 0$ , is equal to  $-1$ .

#### 5.4.4 Linear Complexity Computation

This section gives bounds on LC of GGMW sequences. The linear complexity of a sequence  $S = \{s_i\}$  is the smallest  $r^{\text{th}}$  degree linear recursion satisfied by  $S$  exists. We make use of generalized Blahut's theorem for finding the linear complexity of sequences over residue class rings given in Section 2.5.3. If  $S = \{s_i\}$  is a sequence over  $Z_4$  of period  $2^r-1$ , then from Theorem 2.5.5, the LC of  $S$  is determined by expanding  $s_i$  in the form

$$s_i = \sum_{j=0}^{2^{ru}-2} s_j \alpha^j, i \in Z_{2^{ru}-1}, \quad (5.4.5)$$

where  $\alpha$  is primitive in  $G_c \in \text{GR}(4, ru)$ , and counting number of non zero coefficients in the expansion.

$$LC(\{s_i\}) = |\{\tilde{s}_j: \tilde{s}_j \neq 0, j \in Z_{2^{ru}-1}\}| \quad (5.4.6)$$

where  $|\{\cdot\}|$  represents the cardinality of the enclosed set.  $\tilde{s}_j$ 's are determined by

$$\tilde{s}_j = \sum_{i=0}^{2^{ru}-2} s_i \alpha^{-ji}, j \in Z_{2^{ru}-1} \quad (5.4.7)$$

Following lemmas are useful in evaluating LC properties of GGMW sequences over  $Z_4$ .

**Lemma 5.4.3:** Let  $S = \{s_i\}$  be a sequence over  $Z_4$ . Let  $2S$  be a sequence obtained from  $S$  by multiplying 2 to all elements of  $S$ ;  $2S = \{2s_i\}$ . Then the LC of  $2S$  is always less than or equal to that of  $S$ .

**Proof:** From (5.4.7), nonzero Fourier transform coefficients of  $2S$  is obtained by multiplying 2 to that of  $S$ . Since 2 is a zero divisor, for any  $x$ ,  $2x$  can be either 0 or zero divisor. Hence number of nonzero transform values of  $2S$  is less than or equal to that of  $S$ . Result then follows from Theorem 2.5.5.  $\square$

**Lemma 5.4.4:** Let  $S^A = \{s_i\}$  be a sequence over  $Z_4$  and whose elements are given by

$$s_i = \text{tr}_1^r([\text{tr}_r^{ru}(A\alpha^i)]^{\text{power } b}) \quad (5.4.8)$$

where  $\alpha$  is a primitive in  $G_c$  and  $0 < b < 2^r - 1$ ,  $(b, 2^r - 1) = 1$ . Then the LC of  $S^A$  is given by

$$LC(S^A) = r(u^{H(b)}) \quad (5.4.9)$$

**Proof:** Since  $2S^A = S^2$  which is isomorphic to binary GMW sequence,  $LC(2S^A)$  is given by  $r(u^{H(b)})$  (refer (5.2.6)). Hence from Lemma 5.4.3,  $LC(S^A) \geq r(u^{H(b)})$ . Thus it is sufficient if we show that  $LC(S^A) \leq r(u^{H(b)})$ . Exponent  $b$  of the permutation monomial can be written as  $b = \sum_{i=1}^{H(b)} 2^{d_i}$ , where  $d_i$ 's are distinct integers in the range  $0 \leq d_i < r$  for all  $i$ . Hence (5.4.8) can be written as

$$s_i = \text{tr}_1^r\left(\prod_{i=1}^{H(b)} \sigma^{d_i} [\text{tr}_r^{ru}(A\alpha^i)]\right).$$

By expanding the inner and outer trace, the above expression can be written as linear sum of various powers of  $\alpha$ . The maximum number of powers of  $\alpha$  present in the above expression is  $r(u^{H(b)})$ . Hence  $LC(S^A) \leq r(u^{H(b)})$ .  $\square$ .

Lemma 5.4.5 is a property concerned with binary GMW sequence and it is used in subsequent lemmas.

**Lemma 5.4.5:** Let  $S = \{s_i\}$  be a field sequence defined by  $s_i = [\text{tr}_r^{ru}(\alpha^i)]$ , where  $\alpha$  is primitive in  $GF(2^{ru})$  ( $S$

is a intermediate sequence of GMW sequence over  $Z_2$  of period  $2^{ru}-1$ ). Let  $T = \frac{(2^{ru}-1)}{(2^r-1)}$ , then every

segment of  $T$  consecutive elements from  $S$  contains exactly  $\frac{(2^{(r-1)u}-1)}{(2^r-1)}$  zeros.

Proof: The field element  $\alpha^T$  has order  $2^r-1$ , and hence belongs to  $\text{GF}(2^r)$  a subfield of  $\text{GF}(2^{ru})$ . Then using trace property A10 (Appendix A), for any integer  $n$  we have

$$\text{tr}_r^{ru}(\alpha^i) = \alpha^{-nT} \text{tr}_r^{ru}(\alpha^{i-nT}). \quad (5.4.10)$$

Since  $\alpha^{-nT}$  is not zero, the trace functions in (5.4.10) must be zero for some values of  $i$ . Hence zero locations in  $\{b_i\}$  follow a  $T$  periodicity. Trace property A11 (Appendix A) indicates that there are  $2^{ru-r}-1$  zeros in one period i.e.,  $(2^r-1)T$  symbols of  $\{b_i\}$ . Thus the number of zeros in first  $T$  positions is given by  $(2^{(u-1)r}-1)/(2^r-1)$ .  $\square$

Lemma 5.4.6: Let  $\hat{S}^A = \{s_i'\}$  be an intermediate sequence over  $\text{GR}(4,r) \in \text{GR}(4,ru)$  given by

$$s_i' = [\text{tr}_r^{ru}(A\alpha^i)]$$

where  $\alpha$  is primitive in  $G_c$ . Let  $T = \frac{(2^{ru}-1)}{(2^r-1)}$ , then every segment of  $T$  consecutive elements from  $\hat{S}^A$  contains exactly  $\frac{(2^{(r-1)u}-1)}{(2^r-1)}$  elements from  $\langle 2 \text{ GR}(4,r) \rangle$ .

Proof: Observe that  $2\hat{S}^A$  is isomorphic to a sequence over  $\langle 2 \text{ GR}(4,r) \rangle \cong \text{GF}(2^r)$ . Thus, every segment of  $T$  consecutive elements in  $2\hat{S}^A$  contains exactly  $(2^{(r-1)u}-1)/(2^r-1)$  zeros (Lemma 5.4.5). The result then follows since  $2s_i'$  is zero if and only if  $s_i' \in \langle 2 \rangle$  (P4 of Chapter3).  $\square$

Lemma 5.4.7: Let  $S^A = \{s_i\}$ ;  $A \in \text{GR}(4,ru)$ , be a sequence over  $\text{GR}(4,r)$  defined as follows

$$s_i = \Psi'[\text{tr}_r^{ru}(A\alpha^i)]$$

where  $\Psi'$  is a mapping defined by

$$\begin{aligned} \Psi'(x) &= 2(x_u)^b \text{ whenever } x \text{ is a zero divisor } x = 2x_u \\ &= 0 \text{ whenever } x \text{ is unit} \end{aligned}$$

Then the LC of the sequence  $S$  is upper bounded by  $\frac{(2^{ru}-1)}{(2^r-1)}$  and non-zero positions in the fourier transform representation of  $S^A$  (refer (5.4.5)) belong to the set

$$\{b, b+R, b+2R, \dots, b+(T-1)R\}; R = 2^{r-1}.$$

Proof: Let  $S(x)$  be a polynomial associated with a sequence  $S^A$  given by

$$S(x) = s_0 + s_1x + \dots + s_{L-1}x^{L-1}, L = 2^{ru}-1.$$

Let  $s_{i_1}, s_{i_2}, \dots, s_{i_t}$  be non-zero positions in first  $T$  locations of  $S$ . Here also  $s_i$ 's follow  $T$  periodicity similar to



(5.4.10). Thus by using the definition of  $s_i$ 's  $S(x)$  can be written as

$$S(x) = \hat{S}(x) + x^T(\alpha^{Tb} \hat{S}(x) + \dots x^{(2^r-2)T}(\alpha^{(2^r-2)Tb} \hat{S}(x))) \quad (5.4.11)$$

where  $\hat{S}(x) = s_{i_1} x^{i_1} + s_{i_2} x^{i_2} + \dots + s_{i_t} x^{i_t}$ , is polynomial with maximum of  $\frac{(2^{(r-1)u}-1)}{(2^r-1)}$  non zero coefficients and of degree  $< T$ . From (5.4.5) and (5.4.6) the LC of  $S$  is equal to number of nonzero roots  $\alpha^{-j}$ ,  $j = 0, 1, \dots, 2^{ru}-2$  of  $S(x)$ ;  $\alpha$  is primitive element of  $G_a \in GR(4, r)$ . Consider an evaluation of  $S(x)$  for some  $\alpha^{-j}$ . From (5.4.11),  $S(\alpha^{-j})$  is given by

$$S(\alpha^{-j}) = \partial + \alpha^{T(b-j)} \partial + \alpha^{2T(b-j)} \partial + \dots + \alpha^{(2^r-2)T(b-j)} \partial \quad (5.4.12)$$

Where  $\partial = \hat{S}(\alpha^{-j})$ . When  $j = b' + nR$ ,  $0 \leq n < T$ ,  $b' \neq b$ , then  $S(\alpha^{-j})$  is given by  $S(\alpha^{-j}) = \partial(1 + \alpha^{T(b-b')} + \alpha^{2T(b-b')} + \dots + \alpha^{(2^r-2)T(b-b')})$ . Since  $\partial$  is a zero divisor  $S(\alpha^{-j})$  is the sum of all elements of  $< 2GR(4, r) >$  which is always 0, since  $< 2GR(4, r) >$  is isomorphic to  $GF(2^r)$  (sum of all nonzero elements of  $GF(2^r)$  is always 0). When  $j = b + nR$ ,  $0 \leq n < T$ ,  $S(\alpha^{-j})$  becomes  $(2^{ru}-1)\partial$  which is non-zero if and only if  $\partial$  is non-zero since  $2^{ru}-1$  is a unit in  $Z_4$ . Thus the non-zero roots of  $S(x)$  can at most be  $T$ . Result then follows from (5.4.6).  $\square$

**Theorem 5.4.2:** The LC of a GGMW $^{\Psi_2}$  sequences (when monomial of second type is used ( $\Psi_2^b$ ) to permute intermediate ring  $GR(4, r)$ ) belongs to the range

$$\{r(u)^{H(b)}, \dots, r(u)^{H(b)} - \frac{(2^{ru}-1)}{(2^r-1)} r\}$$

**Proof:** First level GGMW sequence is isomorphic GMW sequence over  $GF(2)$  and hence its LC is equal to  $r(u)^{H(b)}$ . LC of zeroth level sequences is calculated as follows. Since the monomial mapping  $\Psi_2$  is different for units and zero divisors, any sequence  $S^A \in GGMW^{\Psi_2}$ , can be written as sum of two sequences:

$$\begin{aligned} s_i^A &= \text{tr}_1^r(\Psi[\text{tr}_r^{ru}(A\alpha^i)]) = S^1 + S^2 \\ &= \text{tr}_1^r(\{\text{tr}_r^{ru}(A\alpha^i)\}^{\text{power}(b)}) + \text{tr}_1^r(\Psi'[\text{tr}_r^{ru}(A\alpha^i)]) \end{aligned}$$

where  $\Psi'$  is a mapping as defined in Lemma 5.4.5. From Lemmas 5.4.4 and lemma 5.4.5, LC of the first sequence is  $r(u)^{H(b)}$ , and that of second is bounded by  $\frac{(2^{ru}-1)}{(2^r-1)} r$ . Since the non-zero transform position of the first sequence  $\alpha^{-b}$  coincides with that of second, the maximum achievable LC of  $S^A$  is  $\frac{(2^{ru}-1)}{(2^r-1)} r - r(u)^{H(b)}$  as required.  $\square$

When permutation monomials of the first type ( $\Psi_1$ ) are used in the construction GGMW sequences, LC computation done in the Theorem 5.4.2 no longer holds. However a GGMW $^{\Psi_1}$  sequence  $S^A$ ,  $A \in \text{GR}(4, ru)$  can again be split up in to two sequences given by

$$s_i^A = \text{tr}_1^r(\Psi_1[\text{tr}_r^{ru}(A\alpha^i)]) = \text{tr}_1^r(\{\text{tr}_r^{ru}(A\alpha^i)\}^b) + \text{tr}_1^r(\Psi'[\text{tr}_r^{ru}(A\alpha^i)]), \quad (5.4.13)$$

where  $b$  is in the range  $1 \leq b < 2(2^r-1)$  and  $\Psi'$  as defined in Lemma 5.4.5. Consider the first sequence of (5.4.13) given by  $\{s_i^b\}$ ,  $s_i^b = \text{tr}_1^r(\{\text{tr}_r^{ru}(A\alpha^i)\}^b)$ .  $2\{s_i^b\}$  is a GMW sequence over  $\langle 2 \rangle$ , and its LC is given by  $r(u)^{H(b')}$ , where  $b' = b \bmod 2^r-1$  and  $H(b')$  is the number of ones in the binary representation of  $b'$ . Thus from Lemma 5.4.3,  $\text{LC}(S^A) \geq r(u)^{H(b')}$ . Unlike in the case of monomial of second type ( $\Psi_2$ ), we can only give here a lower bound on LC due to difficulty in expressing  $\Psi_1^b$  in terms of  $\Psi_2^b$ . However computer results indicate that LC of GGMW $^{\Psi_1}$  sequences is of the same order as that GGMW $^{\Psi_2}$  sequences.

*Example 5.4.3:* GMW $^{\Psi_2}$  sequences of period 4095;  $r = 6$ ,  $u = 2$ , and power polynomial permutation is  $x \rightarrow x^7$ . Maximum achievable LC is  $65*6 + 8*6 = 438$ .

*Example 5.4.4:* GMW sequences over  $Z_4$  of period 63;  $r=3$ ,  $u=2$ . LC properties of some families are given in Table 5.4.5.

Table 5.4.2 Linear Complexity Properties of GGMW Sequences of Period 63

Permutation	$b$	Linear complexity
$\Psi_1$	3	$\{27, 12\}$
$\Psi_1$	5	$\{12, 21, 27, 18\}$
$\Psi_1$	9	$\{6, 12, 18, 27\}$
$\Psi_1$	11	$\{6, 12, 27, 24\}$
$\Psi_1$	13	$\{12, 18, 27\}$
$\Psi_2$	1,2,3	$\{6\}$

## 5.5 Properties of Families of GGMW Sequences over $P_p^n[w]$

This section gives Hamming correlation and LC properties of a subset of zeroth level GGMW sequences over  $P_p^n[w^k]$ . Let  $\hat{S}^A = \{s_i\}$  be a zeroth level GGMW sequence associated with  $A \in G_a$  of  $\text{PGR}^*(V^k, ru)$ , given by

$$s_i = \text{tr}_1^r(\Psi^b[\text{tr}_r^{ru}(A\alpha^i)]), i \in Z_{Vru-1} \quad (5.5.1)$$

where  $\Psi^b(\cdot)$  is a generalized permutation monomial over  $\text{PGR}(V^k, r)$  as defined in Section 5.1.2. By using the ideal representation of  $G_a$  over  $\text{SP}_p^m[w]$ ,  $A \in G_a$  of  $\text{PGR}^*(V^k, ru)$  can be written as

$$A = 1 + w(A'_0 + A'_1 w + \dots + w^{k-2} A'_{k-1}), \text{ where } A'_i \in \{G_c, 0\} = \text{SPGR}(V, ru) \quad (5.5.2)$$

Then (5.5.1) becomes

$$s_i = \text{tr}_1^r(\Psi[\text{tr}_r^{ru}((1 + wA'_0 + w^2 A'_1 + \dots + w^{k-2} A'_{k-1}) \alpha^i)]), i \in Z_{Vru-1}. \quad (5.5.3)$$

Thus  $j^{\text{th}}$  component sequence in the ideal basis representation,  $1 \leq j \leq k$ ,  $\{s_{i,j}, i \in Z_{Vru-1}\}$  can be written as

$$s_{i,j} = \text{tr}_1^r([\text{tr}_r^{ru}(A'_{j-1} \alpha^i)]^b), i \in Z_{Vru-1} \quad (5.5.4)$$

where  $A'_{-1} = 1$ , and  $A'_j, j \geq 0$  are as in (5.5.2). Since  $\alpha \in \text{SPGR}(V, ru) = \text{GF}(V^{ru})$ , component sequences of  $\hat{S}^A$  are GMW sequences over  $\text{SP}_p^m[w] = \text{GF}(V)$ . Let  $\mathcal{N}_S(a)$  be number of occurrences of symbol  $a$  in  $S$ . Lemma 5.5.1 relates Hamming correlation transform ( $\mathcal{K}^H$ ) of GGMW sequences to that of  $m$ -sequences.

**Lemma 5.5.1:** Let  $\hat{S}^A$  be a GGMW sequence over  $P_p^m[w^k]$ . Then  $\mathcal{N}_{\hat{S}^A}(a)$  is equal to number of occurrences of symbol  $a$  in an  $m$ -sequence  $S^A$ . Thus Hamming correlation transform of  $\hat{S}^A$  is same as that of  $m$ -sequence  $S^A$ .

**Proof:** Consider the elements of intermediate sequence  $SI^A$  of the  $m$ -sequence  $S^A$  given by  $\{\text{tr}_r^{ru}(A \alpha^i)$ , for all  $i \in Z_{Vru-1}\}$ . The monomial permutation  $\Psi^b$ , permutes these elements of  $SI^A$ . Thus  $s_i$ 's of (4.5.3) is some permutation of elements of  $m$ -sequence  $S^A$ . Thus  $\mathcal{N}_{\hat{S}^A}(a)$  is equal to  $\mathcal{N}_{S^A}(a)$ . Result then follows from Lemma 4.4.1.  $\square$

From Lemma 5.5.1 it is clear that  $\mathcal{K}^H$  distribution of family of GGMW sequences is same as that of  $m$ -sequences. But the Hamming autocorrelation properties of GGMW sequences is not related to  $\mathcal{K}^H$  alone in view of the fact that  $\Psi^b$  is a non-linear permutation on  $\text{PGR}(V^k, r)$ . We consider a subset of GGMW sequences which has optimal Hamming autocorrelations properties.

### 5.5.1 Hamming Correlation Computation of a Subgroup of GGMW Sequences

Let  $G'_a$  and  $G'_c$  be the Abelian and cyclic component groups of group of units of subring  $\text{PGR}^*(V^k, r) \in \text{PGR}^*(V^k, ru)$ . Let  $\mathcal{J}$  a subset of GGMW sequences given by  $\mathcal{J} = \{S^A, A \in G'_a\}$ . Using D.5 of Appendix D and ideal basis representation,  $A \in G'_a$ , can be written as

$A = 1 + w(A'_0 + A'_1 w + \dots + w^{k-2} A'_{k-1})$ , where  $A'_i \in \{G'_c \cup 0\} = \text{SPGR}(V, r)$  of  $\text{PGR}^*(V^k, r)$ . Then from (5.1.8) and a trace property (D16 of Appendix D),  $j^{\text{th}}$  componet sequence of  $S^A \in \mathcal{J}, j = 0, \dots, k-1, \{s_{i,j}, i \in Z_{Vru-1}\}$  is given by

$$s_{i,j} = (\text{tr}_1^r(A_{j-1}^i))^b [\text{tr}_r^{ru}(\alpha^i)]^b, i \in Z_{V^{ru}-1}. \quad (5.5.5)$$

where  $A_{-1} = 1$ . Since  $\alpha \in \text{SPGR}(V, ru) = \text{GF}(V^{ru})$ ,  $\text{tr}_r^{ru}(\alpha^i)$  for  $i \in Z_{V^{ru}-1}$  belongs to  $\text{SPGR}(V, r) = \text{GF}(V^r)$ .

Lemmas 5.5.2 to 5.5.5 are used to compute autocorrelation properties of GGMW sequences belonging to  $\mathcal{G}$ . Let  $\hat{S}^A = \{s_i\}$  be a GGMW sequence over  $P_p^n[w^k]$  belonging to the set  $\mathcal{G}$ . Let  $SD^j$ ,  $j = 0, 1, \dots, T-1$ , be decimated sequences of  $S^A$  given by  $SD^j = \{s_i^j, 0 \leq i < V^r-1\}$ ;  $s_i^j = s_{(j+i \cdot T)}$ , where  $T = \frac{(2^{ru}-1)}{(2^r-1)}$ .

**Lemma 5.5.2:** Decimated sequence  $SD^j$ ,  $j = 0, 1, \dots, T-1$ , is a  $m$ -sequence of period  $V^r-1$  given by  $SD^j = S^{\eta_j}$ , where  $\eta_j = [\text{tr}_r^{ru}(\alpha^j)]^b \Psi(A)$

**Proof:** Follows from the definition of  $SD^j$  and  $\hat{S}^A$ .

Let  $D(\tau) = \{d_i\}$  be the point wise subtraction of  $\tau^{\text{th}}$  shift of GGMW sequence  $\hat{S}^A$  from  $\hat{S}^A$ ,  $\hat{S}^A \in \mathcal{G}$ , then decimated sequences  $D^j(\tau)$ , of  $D(\tau)$ ,  $j = 0, 1, \dots, T-1$ , are given by  $D^j(\tau) = \{d_i^j, i \in Z_{V^r-1}\}$ ;  $d_i^j = d_{(j+i \cdot T)}$ , where  $T = \frac{(2^{ru}-1)}{(2^r-1)}$ .

**Lemma 5.5.3:** Decimated sequence  $D^j(\tau)$ , of  $D(\tau)$ ,  $j = 0, 1, \dots, T-1$ , is given by a  $m$ -sequence of period  $V^r-1$ ;  $D^j(\tau) = S^{\eta_j}$ , where  $\eta_j = \delta(j, \tau) \Psi(A)$ ,  $\delta(j, \tau) = ([\text{tr}_r^{ru}(\alpha^j)]^b - [\text{tr}_r^{ru}(\alpha^{j+\tau})]^b)$ .

**Proof:** From the definition of  $\Psi$  and  $\hat{S}^A$ .

**Lemma 5.5.4:**  $\mathcal{K}_{D(\tau)}(a) = \mathcal{K}_{MD(\tau)}(a)$ ,  $a \in P_p^n[w^k]$ , where  $MD(\tau)$  is the point wise subtraction of  $m$ -sequence  $S^{\Psi(A)}$  from  $\tau^{\text{th}}$  shift of  $S^{\Psi(A)}$ .

**Proof:** When  $\tau = 0$ , the result is trivially true since both  $D(0)$  and  $MD(0)$  are all-zero sequences. Let  $\tau \neq 0$ . From the definition of  $m$ -sequences,  $j^{\text{th}}$  decimated sequence of  $MD(\tau)$ ,  $MD^j(\tau)$ , is given by  $S^{\eta_j^*}$ , where  $\eta_j^* = \delta^*(j, \tau) \Psi(A)$ ,  $\delta^*(j, \tau) = ([\text{tr}_r^{ru}(\alpha^j)] - [\text{tr}_r^{ru}(\alpha^{j+\tau})])$ .  $\delta^*(j, \tau)$  and  $\delta(j, \tau)$  are simultaneously zero or non-zero since  $b$  is relatively prime to  $2^r-1$  which is the order of the  $\text{SPGR}^*(V, r)$ . Thus  $D^j(\tau)$  is a some permutation of  $MD^j(\tau)$ . The result then follows immediately.  $\square$

Since  $m$ -sequences are linear sequences,  $MD(\tau)$  is also an another  $m$ -sequence. Thus  $\mathcal{K}_{D(\tau)}(a)$  of  $D(\tau)$  has been related the weight properties of  $m$ -sequences which have been computed in Chapter 4. Lemma 5.5.5 and Theorem 5.5.1 are the immediate consequences of this relation.

**Lemma 5.5.5:** Let  $\mathcal{R}(\Psi(A)) = \rho$ , then  $\mathcal{K}_{D(\tau)}(a)$  for decimated sequence  $D(\tau)$ ,  $\tau \neq 0$ , is given by

$$\begin{aligned}\mathcal{K}_{D(\tau)}(a) &= V^{(ru)-\rho}-1, \text{ for } a = 0 \\ &= V^{(ru)-\rho}, \text{ for } \tau \neq 0\end{aligned}$$

**Proof:** Result follows from Lemmas 5.5.4 and 4.4.5.  $\square$

**Theorem 5.5.1:** Let  $\mathcal{R}(\Psi(A)) = \rho$ , then Hamming autocorrelation function  $H_A(\tau)$  is given by

$$\begin{aligned}H_A(\tau) &= V^{ru}-1, \text{ for } \tau = 0 \\ &= V^{(ru)-\rho}-1 \text{ for } \tau \neq 0\end{aligned}$$

**Proof:** From Lemmas 5.5.5 and 4.4.1.  $\square$

## 5.5.2 Construction of Optimal Families of Sequences from GGMW Sequences over $P_p^n[w^k]$

Let  $\hat{S}^A = \{s_i\}$  be a GGMW sequence over  $P_p^n[w^k]$  belonging to  $\mathcal{J}$ , then for every  $\gamma \in \text{Trace image of } \hat{S}^A$ , we define a sequence  $\hat{S}^A(\gamma)$  given by  $\{s_i + \gamma, 0 \leq i \leq V^{ru}-1\}$ . Then a family of  $V^\rho$  sequences associated with  $S^A$  is given by the set of sequences  $\{S^A(\gamma), \gamma \in \text{Trace image of } S^A\}$ . We denote such a family by  $\text{GGMW}(A)$ .

**Theorem 5.5.2:** Hamming crosscorrelation between any two sequences in the  $\text{GGMW}(A)$ ,  $S^A(\gamma_1)$  and  $S^A(\gamma_2)$ , is given by

$$\begin{aligned}H_{\gamma_1\gamma_2}(\tau) &= V^{ru-\rho}-1, \text{ whenever } \gamma_1 = \gamma_2 \\ H_{\gamma_1\gamma_2}(\tau) &= V^{ru}-1, \text{ whenever } \gamma_1 = \gamma_2 \text{ and } \tau = 0 \\ H_{\gamma_1\gamma_2}(\tau) &= 0, \text{ whenever } \gamma_1 \neq \gamma_2 \text{ and } \tau = 0. \\ H_{\gamma_1\gamma_2}(\tau) &= V^{ru-\rho}, \text{ whenever } \gamma_1 \neq \gamma_2.\end{aligned}$$

Thus the family  $\text{GGMW}(A)$  is optimal.

Proof: First two results follow from Theorem 5.5.1. When  $\gamma_1 \neq \gamma_2$ ,  $H_{\gamma_1\gamma_2}(0)$  is given by  $\mathcal{K}_{D(0)}(\gamma_1 - \gamma_2)$  which is zero since  $D(0)$  is all-zero sequence. For  $\tau \neq 0$ ,  $H_{\gamma_1\gamma_2}(\tau)$  from Lemma 4.4.1 is given by  $H_{\gamma_1\gamma_2}(\tau) = \mathcal{K}_{D(\tau)}(0^k)$ , where  $D(\tau) = S^A(\gamma_1) - T^\tau(S^A(\gamma_2))$ . This can be written as  $\mathcal{K}_{D'}(\gamma_1 - \gamma_2)$ , where  $D' = S^A - S^A \alpha^\tau$ , using the definition of m-sequences. Result then follows From Lemma 5.5.5. From (2.5.8) and (2.5.9), the family GGMW( $A$ ) is optimal according to Lempel and Greenberger bound on  $H_{\max}$ .  $\square$

### 5.5.3 Sets of Frequency Hopping Patterns from Optimal Families of GGMW( $A$ ) Sequences

Construction of frequency hopping patterns from GGMW( $A$ ) sequences is similar to the procedure given in Chapter 4. Each symbol  $a$  in the ring  $P_p^n[w^k]$  is associated with a distinct frequency belonging to the frequency library. Schematic diagram of generating frequency hopping patterns from GGMW sequences over  $P_p^n[w^k]$  is given in Fig 5.5.1. Basis selector chooses linearly independent component sequences of  $\hat{S}^A$ .

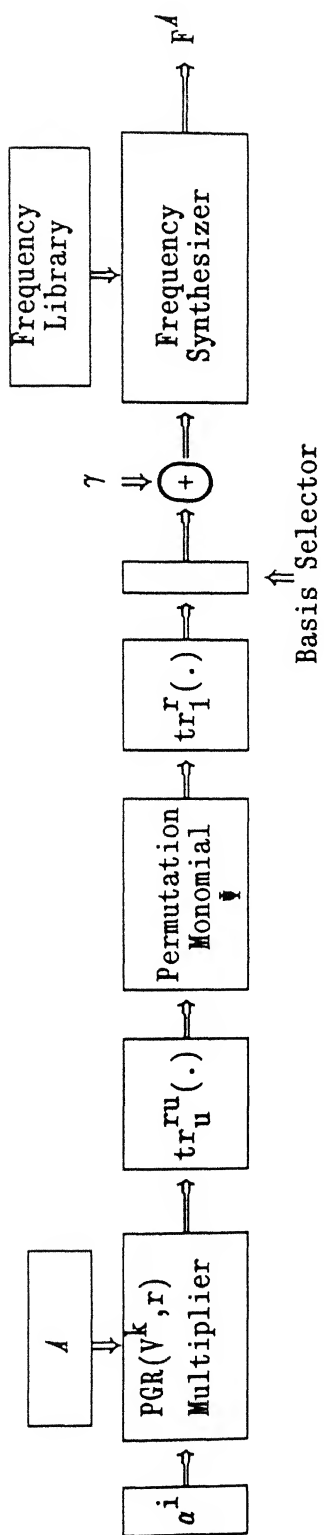
Now it remains to compute number of GGMW( $A$ ) families. Similar to  $\mathcal{K}$  here also corresponding to every GGMW-sequence  $S^A$  belonging to  $\mathcal{J}$ , a family of frequency hopping sequences are constructed and the correlation properties depends on the rank number of  $\Psi(A)$ . Hence, corresponding to a distinct GGMW family there are  $\#(r, \rho)$  different frequency hopping families of size  $V^\rho$ . By following similar arguments of Section 5.3, number of distinct GGMW families in this case can be shown to be equal to  $(\phi(2^{ru}-1)/ru)(\phi(r)/r)$ . Thus number of frequency hopping sets of size  $V^\rho$ ,  $1 \leq \rho \leq r$  is given by  $(\phi(2^{ru}-1)/ru) (\phi(r)/r) \#(r, \rho)$ .

### 5.5.4 Linear Complexity of GGMW Sequences $P_p^n[w^k]$

**Lemma 5.5.6:** Let  $\hat{S}^A = \{s_i\}$  be a GGMW sequence associated with  $A \in PGR^*(V^k, ru)$ . Then LC of  $\hat{S}^A$  is equal to the LC of its corresponding sequence over residue field (sequence obtained from  $\hat{S}^A$  by taking modulo  $w$  on each symbol of  $\hat{S}^A$ ).

Proof: From Theorem 2.5.5, the LC of  $\hat{S}^A$  is determined by expanding  $s_i$  in the form

$$s_i = \sum_{j=0}^{V^{ru}-2} s_j \alpha^{ij}, i \in Z_{V^{ru}-1}, \quad (5.5.6)$$



$A \in \text{PGR}(V^k, ru), a \in G_c \text{ of } \text{PGR}(V^k, ru); r, u \text{ are positive integers}$

$\gamma \in \text{PGR}(V^k, r)$

Basis selector chooses linear independent positions of  $\text{PGR}(V^k, r)$  in  $\text{PGR}(V^k, ru)$

Fig 5.5.1 Schematic Diagram of Generation of Frequency Hopping Patterns  
from GGMV Sequences over  $P_p^n[v^k]$

where  $\alpha$  is primitive in  $G_c \in \text{PGR}(V^k, ru)$ , and counting number of non zero coefficients in the expansion.

$$\text{LC}(\{s_i\}) = |\{\tilde{s}_j: \tilde{s}_j \neq 0, j \in Z_{Vru-1}\}| \quad (5.5.7)$$

where  $|\{\cdot\}|$  represents the cardinality of the enclosed set.  $\tilde{s}_j$ 's are determined by

$$\tilde{s}_j = \sum_{i=0}^{V^{ru}-2} s_i \alpha^{-ji}, j \in Z_{Vru-1} \quad (5.5.8)$$

Consider  $j^{\text{th}}$  component sequence of  $\hat{S}^A$  and its transform  $\tilde{S}^A$ . From (5.5.8),  $\tilde{s}_j$  is non-zero if and only if one of  $\tilde{s}_{j,m}$  is non-zero,  $0 \leq m < k$ . Non-zero transform coefficient positions of all component sequences are same since same monomial is used for permuting intermediate field elements ( $x \rightarrow x^b$ ). Zeroth component sequence of  $\hat{S}^A$  is the residue field sequence. Thus number of non-zero transform values of  $\hat{S}^A$  is equal to non-zero transform of values of its residue sequence.  $\square$

Thus LC of GGMW sequences is equal to the LC of corresponding GMW sequences. Thus LC of GGMW sequences of period  $2^{ru}-1$  over  $P_2^n[w^k]$  is equal to  $r(u)^{H(b)}$ , where  $b$  and  $H(b)$  are as defined in (5.1.8).

*Example 5.5.1:* GGMW sequence over  $P_2^2[w^2]$ ;  $w = \xi$  generated by  $\alpha \in \text{PGR}(V^2, ru)$ ;  $V = \text{GF}(2)$ ,  $ru=6$ ,  $r=3, u=2$ , such that  $\alpha^6 = \alpha + 1$ . Vectors over  $\text{GF}(2)$  in simple brackets represents  $P_2^2[w^2]$  symbols. A GGMW sequence associated with  $A = [(10)] \in \text{PGR}^*(2^2, 6)$   $S^A$  is given by

$$\begin{aligned} S^A = \{ & (10)(10)(10)(10)(00)(10)(10)(10)(00)(00)(10)(10)(10)(10)(00)(10) \\ & (00)(00)(10)(00)(10)(10)(00)(10)(10)(10)(00)(10)(00)(00)(00)(10) \\ & (10)(00)(10)(00)(10)(10)(00)(00)(10)(10)(00)(10)(00)(00)(00)(10) \\ & (10)(10)(00)(10)(00)(00)(00)(10)(00)(00)(00)(00)(00)(00)(00) \} \end{aligned}$$

The LC of the above sequence is 12.

*Example 5.5.2:* Family of frequency hopping patterns of length 63 derived from a GGMW sequence over  $P_2^2[\xi^2]$ : GGMW( $A$ ). GGMW Sequence is generated by  $\alpha$  such that  $\alpha^6 = \alpha + 1$ ,  $\alpha \in \text{PGR}(V^2, 6)$ , where  $V = \text{GF}(2)$ . Permutation polynomial used to permute intermediate ring  $\text{PGR}(V^2, 3)$  is monomial  $x \rightarrow x^3$ . Patterns are constructed from a GGMW sequence  $S^A$ ,  $A = (10) + (01)\alpha + (01)\alpha^2 + (01)\alpha^3$ .  $\mathcal{R}\mathcal{A}(A)$  is 2. Number of patterns in GGMW( $A$ ) is 4. Elements of  $P_2^2[\xi^2]$  are represented by 2-tuples over  $\text{GF}(2)$ , for example, (11) represents  $1 + \xi$ . The GGMW family  $S^A$  is given by



$$S^A = \{(11)(10)(10)(10)(01)(11)(10)(11)(00)(01)(11)(10)(10)(11)(01)(10)(01)(00)(10)(00)(11)(11)(01)(10)(11)(10)(00)(10)(01)(00)(00)(10)(10)(00)(10)(00)(11)(11)(01)(01)(10)(11)(01)(11)(00)(00)(01)(11)(11)(11)(00)(11)(00)(00)(01)(10)(01)(01)(00)(01)(01)(01)(00)\}.$$

Patterns of the family  $\text{GGMW}((10)+(01)\alpha+(01)\alpha^2+(01)\alpha^3)$  are given in Table 5.5.1. Pattern elements are represented using decimal numbers 0,1,2,3;  $a(\xi)$  of  $P_2^2[\xi^2]$  is represented by decimal number  $a(2)$ .

**Table 5.5.1 Patterns of Family  $\text{GGMW}((10)+(01)\alpha+(01)\alpha^2+(01)\alpha^3)$**

---

Pattern 0 = 311123130231132120103321310120011010332213230023330300212202220

Pattern 1 = 200032021320023031012230201031100101223302321132221211303313331

Pattern 2 = 133301312013310302321103132302233232110031012201112122030020002

Pattern 3 = 022210203102201213230012023213322323001120103310003033121131113

---

## Chapter 6

### Sequences over the Proper Ideal of $Z_4$ with Controllable Linear Complexity

This chapter is concerned with construction of sequences over  $\langle 2 \rangle$ , the proper ideal of  $Z_4$ , through polynomial mappings from  $Z_4$  to  $\langle 2 \rangle$ , and with their biphasic correlation properties. A simple example of such a polynomial mapping is  $\varphi(x) = 2x$ ;  $x \in Z_4$ , which is equivalent to familiar homomorphic mapping  $\varphi(x) = x \bmod 2$ ,  $x \in Z_4$ , from  $Z_4$  to  $Z_2$ . This mapping produces sequences over  $\langle 2 \rangle$  which are structurally similar to corresponding sequences over  $Z_4$  and hence they are not of much importance. In this chapter we consider nonlinear polynomial ( $\mathcal{NLP}$ ) mappings from  $Z_4$  to its ideal  $\langle 2 \rangle$ , which result in structurally different  $\langle 2 \rangle$  sequences from that of  $Z_4$  sequences. The ideal  $\langle 2 \rangle$  is isomorphic to binary field and the quadriphase mapping  $\phi$  (refer (1.2.4)) on the ideal results in biphasic signal set. Thus, families of  $Z_4$  sequences derived in Chapter 3 through  $\mathcal{NLP}$  mappings and the quadriphase mapping ( $\phi$ ) yield biphasic families. The biphasic families thus constructed are named by prefixing the word  $\mathcal{NLP}$  to their corresponding  $Z_4$  families.

Construction of biphasic sequences through transformations from quadriphase to biphasic sequences is not new. Krone and Sarwate [3] have considered one such transformation. Polynomial mappings considered here are similar to the transformation given in [3] which also gives a method of evaluating correlation properties of biphasic sequences and a bound on  $\theta_{\max}$  for biphasic sequences;  $\theta_{\max}(\text{biphasic}) \leq \theta_{\max}(\text{quadriphase})$ . The same correlation evaluation technique is used here also. But, crosscorrelation distributions of biphasic families are computed using the properties of  $\text{GR}(4, r)$  and correlation transform distributions of the corresponding  $Z_4$  families. It is shown that many families are optimal according to Sidelnikov bound ( $\theta_{\max} \leq \sqrt{2L}$ ) and Welch bound ( $\theta_{\max} \leq \sqrt{L}$ ), where  $L$  is the period of the sequences.

Another interesting feature of biphasic sequences given here is their large linear complexity (LC) property. This follows from the nonlinear nature of polynomial functions considered. Generalized Blahut's theorem (Theorem 2.5.5) for computing LC of sequences over  $Z_4$  is used to compute LC of resultant ideal sequences. The LC of biphasic sequences derived here is quadratic in  $r$ , where  $r$  is the degree of extension ring used to define sequences.

The chapter is organized as follows. Section 6.1 gives nonlinear polynomial mappings from  $Z_4$  to  $\langle 2 \rangle$ . Section 6.2 gives correlation expressions for biphase sequences in terms of correlation values of their corresponding  $Z_4$  sequences. Sections 6.3 and 6.4 discuss definitions and properties of families of biphase sequences derived from  $\mathcal{K}$  and  $\mathcal{JK}$  families of  $Z_4$  sequences respectively. LC of the sequences are computed in Section 6.5. Comparison of new families of biphase constructions with known families is given in Section 6.6.

## 6.1 Polynomial Mappings from $Z_4$ to $\langle 2 \rangle$

Polynomial function  $\varphi(x) = 2x$ ,  $x \in Z_4$ , is equivalent to homomorphic mapping  $\varphi(x) = x \bmod 2$ ,  $x \in Z_4$ , from  $Z_4$  to  $Z_2$ , which results in structurally equivalent binary sequences. Two other nontrivial functions are  $\varphi_1(x) = x^2 - x$  and  $\varphi_2(x) = x^2 + x$ . These were found by trial and error and one can verify that they are indeed mappings from  $Z_4$  to  $\langle 2 \rangle$ . The above mentioned mappings are summarized in Table 6.1.1.

Table 6.1.1 Table of Mappings from  $Z_4$  to  $\langle 2 \rangle \equiv \text{GF}(2)$

$u$	$\hat{u}$	$\varphi_1$	$\varphi_2$	$\varphi_3$	$\hat{\varphi}_1$	$\hat{\varphi}_2$	$\hat{\varphi}_3$
0	1	0	0	0	1	1	1
1	$\omega$	0	2	2	1	-1	-1
2	-1	2	2	0	-1	-1	1
3	$-\omega$	2	0	2	-1	1	-1

$$u \in Z_4, \hat{u} = \omega^u; \omega = \sqrt{-1}$$

$$\varphi_1(u) = u^2 - u; \varphi_2(u) = u^2 + u; \varphi_3(u) = 2u;$$

It is easy to verify the following lemma.

**Lemma 6.1.1:** The polynomial mappings  $\varphi_1$ ,  $\varphi_2$  and  $\varphi_3$  given above are the only three mappings with the following two conditions imposed on the definition of mapping:

1. Element '0' of  $Z_4$  has to map to '0' of  $\langle 2 \rangle$ ;  $\varphi(0) = 0$ .
2.  $|\varphi(x)=0| = |\varphi(x)=2|$ .

Where  $|\cdot|$  represents number of solutions of  $(\cdot)$ .

Polynomial functions  $\varphi_1(x)$  and  $\varphi_2(x)$  generate equivalent binary signal sets from a family of sequences  $\phi$  over  $Z_4$ , having a property that if  $S \in \phi$ , then  $3S \in \phi$ , since if  $S \in \phi$ ,  $\varphi_1(S) = \varphi_2(3S)$ . Since the  $Z_4$  families derived in Chapter 3 have this property, only one of the functions  $\varphi_1$  is considered. Hereafter it is denoted by  $\varphi$ .

## 6.2 Correlation Expressions for Biphase Sequences

Let  $\phi$  be the quadriphase mapping given by  $\phi(x) = \omega^x$ ,  $\omega = \sqrt{-1}$ . Let  $U = \{u_i\}$  be a sequence over  $Z_4$  and let  $W$  and  $X$  be two polynomial sequences of  $U$  given by  $w_i = \varphi(u_i)$  and  $x_i = \varphi(3u_i)$ ;  $W$  and  $X$  are sequences over the ideal  $\langle 2 \rangle$ . Since the mapping  $\phi$  maps the  $\langle 2 \rangle$  to biphase signal set  $\{1, -1\}$ ,  $\phi(W)$  and  $\phi(X)$  are biphase sequences. Then it can be verified that

$$\phi(u_i) = \frac{1}{2}(1+\omega)\phi(w_i) + \frac{1}{2}(1-\omega)\phi(x_i). \quad (6.2.1)$$

Thus a sequence over  $Z_4$  can always be split into two biphase sequences, and, conversely given any two biphase sequences it is possible to construct a quadriphase sequence. A  $Z_4$  sequence  $U$  and its corresponding polynomial sequences  $W$  and  $X$  as in (6.2.1) is denoted by  $U = [W, X]$ . Let  $U = [X_1, Y_1]$  and  $V = [X_2, Y_2]$  are two sequences over  $Z_4$  of period  $L$ . Then, it is easily verified that

$$C_{UV}(\tau) = \frac{1}{2}[C_{X_1X_2}(\tau) + C_{Y_1Y_2}(\tau)] + \frac{1}{2}\omega[C_{X_1Y_2}(\tau) - C_{Y_1X_2}(\tau)], \quad (6.2.2)$$

$$C_{UU}(\tau) = \frac{1}{2}[C_{X_1X_1}(\tau) + C_{Y_1Y_1}(\tau)] + \frac{1}{2}\omega[C_{X_1Y_1}(\tau) - C_{Y_1X_1}(\tau)], \quad (6.2.3)$$

where  $C_{AB}(\tau)$  represents crosscorrelation function between  $A$  and  $B$ ;

Also from (6.2.1), note that if  $U = [X_1, Y_1]$  then  $3U = [Y_1, X_1]$ ; hence

$$C_{3U,V}(\tau) = \frac{1}{2}[C_{X_1Y_2}(\tau) + C_{Y_1X_2}(\tau)] + \frac{1}{2}\omega[C_{Y_1Y_2}(\tau) - C_{X_1X_2}(\tau)] \quad (6.2.4)$$

$$C_{3U,U}(\tau) = \frac{1}{2}[C_{Y_1X_1}(\tau) + C_{X_1Y_1}(\tau)] + \frac{1}{2}\omega[C_{Y_1Y_1}(\tau) - C_{X_1X_1}(\tau)]. \quad (6.2.5)$$

Solving the above equations we get

$$C_{X_1X_2}(\tau) = \text{Re}(C_{UV}(\tau)) - \text{Im}(C_{3U,V}(\tau)) \quad (6.2.6)$$

$$C_{X_1X_1}(\tau) = \text{Re}(C_{UU}(\tau)) - \text{Im}(C_{3U,U}(\tau)) \quad (6.2.7)$$

where  $\text{Re}(x)$  and  $\text{Im}(x)$  represent real and imaginary part of  $x$  respectively. Thus from (6.2.6) and (6.2.7),

$\theta_{\max}$  for transformed biphase family becomes

$$\theta_{\max}(\text{BP}) \leq 2\theta_{\max}(\text{QP}), \quad (6.2.8)$$

where QP and BP represents quadriphase and its corresponding biphasic families.

Lemma 6.2.1 gives crosscorrelation between  $\mathcal{NLSP}$  functions of m-sequences and Im-sequences using the correlation identities given above.

**Lemma 6.2.1:** Let  $\varphi(S^a)$  and  $\varphi(S^b)$  be two  $\mathcal{NLSP}$  sequences corresponding to m-sequences or I-msequences  $S^a$  and  $S^b$  respectively. Then crosscorrelation between them is given by

$$C_{\varphi(S^a)\varphi(S^b)}(\tau) = \text{Re}(\kappa(S^{a-b}\alpha^\tau)) - \text{Im}(\kappa(S^{3a-b}\alpha^\tau)).$$

**Proof:** The proof follows from (6.2.6) and the linearity property of m-sequences and Im-sequences.  $\square$

### 6.3 Families of $\mathcal{NLSP}$ Sequences Derived from $\mathcal{K}$ Families over $Z_4$

In this section we consider  $\mathcal{NLSP}$  functions of m-sequence families. The corresponding binary families are denoted by  $\mathcal{K}$ - $\mathcal{NLSP}$ . Schematic diagram of generation of biphasic sequences through  $\mathcal{NLSP}$  mapping from  $Z_4$  to  $\langle 2 \rangle$  is given in Fig 6.3.1.

#### 6.3.1 Weight Distribution of $\mathcal{K}$ - $\mathcal{NLSP}$ Family

Weight distributions of ( $\mathcal{NLSP}$ ) families are computed from the correlation transform distributions of corresponding  $Z_4$  families. Let  $A$  be a  $Z_4$  sequence with weight vector  $W_A$ , then weight vector of transformed polynomial sequence  $\varphi(A)$  is given by  $W'_A$

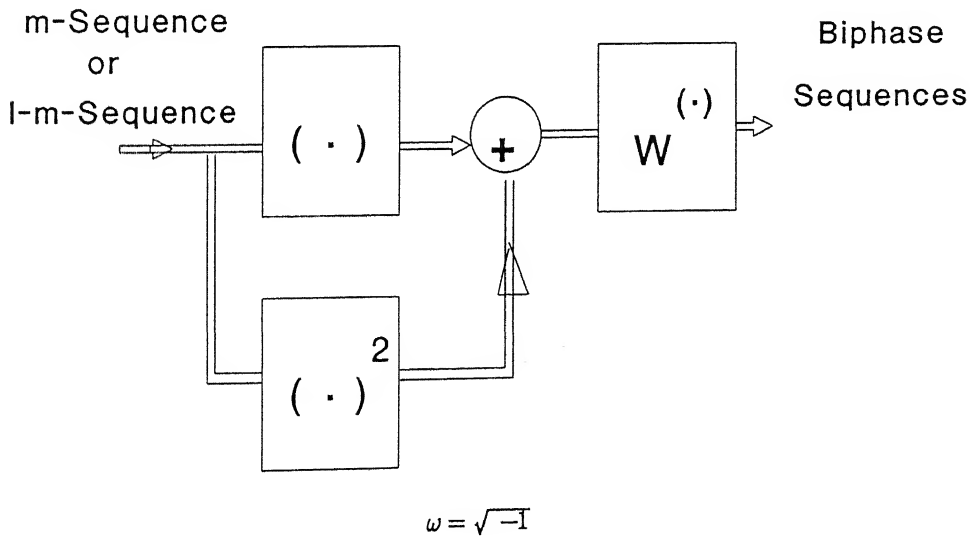


Fig 6.3.1 Schematic Diagram for Generation of Biphasic Sequences from Sequences Over  $Z_4$

$$w'_0 = w_0 + w_1 \quad (6.3.1)$$

$$w'_2 = w_2 + w_3 \quad (6.3.2)$$

$$w'_1 = w'_3 = 0. \quad (6.3.3)$$

since under  $\varphi$ , elements 0, 1 are mapped to 0 and elements 2, 3 are mapped to 2. In view of (6.3.3),  $\aleph$  of  $\varphi(A)$  is given by  $(w'_0 - w'_2)$ . This is also referred as sequence imbalance. Thus by using (6.3.1)–(6.3.2) and  $\aleph$  distributions of  $\mathcal{M}$  families given in Chapter 3.0, weight distributions and correlation transform (sequence imbalance) distributions of  $\mathcal{M}$ - $\mathcal{NLP}$  families (of period  $2^r - 1$ , both  $r$  even and odd) can be easily computed. The weight and  $\aleph$  distributions of  $\mathcal{M}$  families over given in Table 6.3.1.

### 6.3.2 Correlation Distribution of $\mathcal{NLP}$ - $\mathcal{M}$

Correlation distribution  $\mathcal{D}$  of  $\mathcal{NLP}$ - $\mathcal{M}$  family is a set of crosscorrelation values of all pairs of sequences in the family; it is given by:

**Table 6.3.1 Weight and Correlation Transform Distributions of  $\mathcal{NLP}$ - $\mathcal{M}$  Family**

(a) Period :  $2^r - 1$ ,  $r$  an Odd Integer;  $r = 2t + 1$

Sl. No.	$w_0$	$w_2$	Imbalance ( $w_0 - w_2$ )	No of sequences
1.	$2^{2t} + 2^t - 1$	$2^{2t} - 2^t$	$2^{t+1} - 1$	$2^{t-1}(2^t + 1)$
2.	$2^{2t} - 2^t - 1$	$2^{2t} + 2^t$	$-(2^{t+1} + 1)$	$2^{t-1}(2^t - 1)$
3.	$2^{2t} - 1$	$2^{2t}$	$-1$	$2^{2t} + 1$

(b) Period :  $2^r - 1$ ,  $r$  an Even Integer;  $r = 2t$

Sl. No.	$w_0$	$w_2$	Imbalance ( $w_0 - w_2$ )	No of sequences
1.	$2^{2t-1} + 2^{t-1} - 1$	$2^{2t-1} - 2^{t-1}$	$2^t - 1$	$2^{t-1}(2^t + 1)$
2.	$2^{2t-1} - 2^{t-1} - 1$	$2^{2t-1} + 2^{t-1}$	$-(2^t + 1)$	$2^{t-1}(2^t - 1)$
3.	$2^{2t} - 1$	$2^{2t}$	$-1$	1

$$\mathcal{D} = \{C_{XY}(\tau), \text{ for all } X, Y \in \mathcal{NLP}\mathcal{M}, 0 \leq \tau \leq L, L:\text{period}\} \quad (6.3.4)$$

$$\mathcal{D} = \{C_{\varphi(S^a), \varphi(S^b)}(\tau), S^a, S^b \in \mathcal{NLP}\mathcal{M}, 0 \leq \tau \leq L, L:\text{period}\}$$

Corresponding to a fixed  $S^a \in \mathcal{NLP}\mathcal{M}$ , let  $\mathcal{D}^a$  be set of correlation values given by

$$\mathcal{D}^a = \{C_{(\varphi(S^a)\varphi(S^b))}(\tau), \text{ for a fixed } S^a \text{ \& for all } S^b \in \mathcal{NLP}\text{-family}, 0 \leq \tau \leq L\} \quad (6.3.5)$$

Then  $\mathcal{D}$  can be written as:

$$\mathcal{D} = \bigcup_{S^a \in \mathcal{NLP}\mathcal{M}} \mathcal{D}^a, \quad (6.3.6)$$

where  $\bigcup$  represents set theoretic union. Using Lemma 6.2.1, the set  $\mathcal{D}^a$  can be written as

$$\mathcal{D}^a = \{\text{Re}(\aleph(S^a - S^{b\alpha^T})) - \text{Im}(\aleph(S^{3a} - S^{b\alpha^T})); \text{ for all } S^b \in \mathcal{NLP}\mathcal{M}, 0 \leq \tau \leq L\}$$

As  $S^b$  runs over all the sequences in the family,  $b\alpha^T$  for  $0 \leq \tau \leq L$  takes all the values of  $\text{GR}(4,r) \setminus \{0\}$ . Thus using the fact that  $\mathcal{M}$  family is linear,  $\mathcal{D}^a$  can be written as

$$\mathcal{D}^a = \{\text{Re}(\aleph(S^{a-B})) - \text{Im}(\aleph(S^{3a-B})); \text{ for all } B \in (\text{GR}(4,r) \setminus \{0\})\}.$$

The additive property of the  $\text{GR}(4,r)$  implies that

$$\{a-B, \text{ for all } B \in \text{GR}(4,r) \setminus \{0\}\} = \{\text{GR}(4,r) \setminus \{a\}\}. \quad (6.3.7)$$

From the representation of  $\text{GR}(4,r)$  (Section 3.1),  $a-B \in \text{GR}(4,r) \setminus \{a\}$  is represented by  $a-B = c\beta$ ,  $c \in \{G_a/\{a\} \cup \{2\} \cup \{0\}\}$  and  $\beta \in G_c$ . As  $(a-B)$  runs through all values of  $\text{GR}(4,r) \setminus \{a\}$ , in the representation  $a-B=c\beta$ ,  $c$  and  $\beta$  takes all values from  $\{G_a/\{a\} \cup \{2\} \cup \{0\}\}$  and  $G_c$  respectively. We have the following lemma.

**Lemma 6.3.1:** If  $a-B = c\beta$ ;  $a \in G_a$ ,  $B \in \text{GR}(4,r) \setminus \{a\}$ ,  $\beta \in G_c$  and  $c \in G_a$ , then  $3a-B = cd\beta$ , where  $d=(1+2\beta^{-1})$ . If  $a-B = 2\beta$ ;  $a \in G_a$ ,  $B \in \text{GR}(4,r) \setminus \{a\}$ ,  $\beta \in G_c$ , then  $3a-B = 2(\beta+1)$ .

**Proof:** Easy to verify.  $\square$

By using Lemmas 6.2.1 and 6.3.1, and (6.3.7),  $\mathcal{D}^a$  becomes:

$$\begin{aligned} \mathcal{D}^a = & \left\{ \begin{aligned} & \{\text{Re}(\aleph(S^{c\beta})) - \text{Im}(\aleph(S^{dc\beta}))\}; \text{ for all } c \text{ \& } \beta, c \in \{G_a, 0\}, \beta \in G_c\} \\ & \cup \{\text{Re}(\aleph(S^{2\beta})) - \text{Im}(\aleph(S^{2(\beta+1)}))\}; \text{ for all } \beta, \beta \in G_c\} \\ & \setminus \{\text{Re}(\aleph(S^a)) - \text{Im}(\aleph(S^{3a}))\} \end{aligned} \right\} \quad (6.3.8) \end{aligned}$$

Now by applying (6.3.6),  $\mathcal{D}$  becomes:

$$\begin{aligned} \mathcal{D} = & \bigcup_{S^a \in \mathcal{NLP}\mathcal{M}} \left\{ \begin{aligned} & \{\text{Re}(\aleph(S^{c\beta})) - \text{Im}(\aleph(S^{dc\beta}))\}; \text{ for all } c \text{ \& } \beta, c \in \{G_a, 0\}, \beta \in G_c\} \\ & \cup \{\text{Re}(\aleph(S^{2\beta})) - \text{Im}(\aleph(S^{2(\beta+1)}))\}; \text{ for all } \beta, \beta \in G_c\} \\ & \setminus \{\text{Re}(\aleph(S^a)) - \text{Im}(\aleph(S^{3a}))\} \end{aligned} \right\} \quad (6.3.9) \end{aligned}$$

The third set in (6.3.9) is  $\aleph$  distribution of the  $\mathcal{NLN}$  which has been computed in Chapter 3. Essentially it remains only to compute the following set  $\mathcal{P}'$ , given by

$$\begin{aligned} \mathcal{P}' = & \{ \text{Re}(\aleph(S^{c\beta})) - \text{Im}(\aleph(S^{dc\beta})) ; \text{ for all } c \& \beta, c \in G_a, \beta \in G_c \} \\ & \cup \{ \text{Re}(\aleph(S^{2\beta})) - \text{Im}(\aleph(S^{2(\beta+1)})) ; \text{ for all } \beta, \beta \in G_c \} \cup \{L\} \end{aligned} \quad (6.3.10)$$

where  $d = (1+2\beta^{-1})$ . Since  $\mathcal{P}'$  for every  $a$  is same,  $\mathcal{D}$  can be written as

$$\mathcal{D} = \{ \mathcal{P}' \}^M \setminus \{ \aleph \text{ values of } \mathcal{NLN} \text{ family} \} \quad (6.3.11)$$

where  $M$  is the number of sequences in the  $\mathcal{NLN}$  family. The 2<sup>nd</sup> set in (6.3.10) takes a correlation value of  $-1$ ,  $2^t - 1$  times, since  $\text{Im}(\aleph(S^{2(\beta+1)})) = 0$ . Mainly it remains only to compute the values in the first set of  $\mathcal{P}'$ . Here as  $\beta$  varies over  $G_c$ ,  $dc$  takes all values of  $G_a$  except  $c$ . The exact values of  $\aleph$  of  $m$ -sequences  $S^a$  for all  $a \in G_a$  is known and given the Table (3.4.2). The sample computation is illustrated below for  $\mathcal{N}$  ( $r$ : odd). Refer Table 3.4.2, when  $c \in \mathcal{P}$ ,  $\aleph(S^c) = (2^t - 1) + \omega(2^t)$  and as  $\beta$  varies over all  $G_c$ ,  $S^{dc}$  takes all the sequences from subsets  $\mathcal{P}$ ,  $\mathcal{Q}$ ,  $\mathcal{R}$ ,  $\mathcal{S}$  except  $S^c$  it self. Hence the correlation value of

$\text{Re}(\aleph(\mathcal{P})) - \text{Im}(\aleph(\mathcal{P})) = -1$  appears  $|\mathcal{P}|(|\mathcal{P}| - 1) = (2^{t-1}(2^t + 1))((2^{t-1}(2^t + 1) - 1))$  times,

$\text{Re}(\aleph(\mathcal{P})) - \text{Im}(\aleph(\mathcal{Q})) = 2^{t+1} - 1$  appears  $|\mathcal{P}||\mathcal{Q}| = (2^{t-1}(2^t + 1))((2^{t-1}(2^t + 1)))$  times,

$\text{Re}(\aleph(\mathcal{P})) - \text{Im}(\aleph(\mathcal{R})) = -1$  appears  $|\mathcal{P}||\mathcal{R}| = (2^{t-1}(2^t + 1))((2^{t-1}(2^t - 1)))$  times,

$\text{Re}(\aleph(\mathcal{P})) - \text{Im}(\aleph(\mathcal{S})) = 2^{t+1} - 1$  appears  $|\mathcal{P}||\mathcal{S}| = (2^{t-1}(2^t + 1))((2^{t-1}(2^t - 1)))$  times.

Similarly the correlation values are computed for  $c \in \mathcal{Q}$ ,  $\mathcal{R}$  and  $\mathcal{S}$ . This way correlation values of  $\mathcal{P}'$  are computed. Then using (6.3.9) the correlation distribution can be computed. For  $\mathcal{NLN}$  ( $r$ : even) similar arguments hold and the results are tabulated in Table (6.3.2).

## 6.4 Families of $\mathcal{NLN}$ Sequences Derived From $\mathcal{NM}$ Families

In this section, we consider non-linear feed forward ( $\mathcal{NLN}$ ) functions of  $m$ -sequence families. The corresponding binary families are denoted by  $\mathcal{NLN-NM}$ . Depending on the nature of  $\mathcal{NM}$  families, following three types of families are considered.

1.  $\mathcal{NLN-NM}^1(\text{tr}(\tilde{\gamma})=1)$  of Period  $2(2^t - 1)$ ,  $r$ : odd and even.
2.  $\mathcal{NLN-NM}^1(\text{tr}(\tilde{\gamma})=0)$  of Period  $2(2^t - 1)$ ,  $r$ : odd and even.
3.  $\mathcal{NLN-NM}^3$  of Period  $2(2^t - 1)$ ,  $r$ : odd and even.



### 6.4.1 Weight and Correlation Transform Distributions

Weight distributions are computed from their corresponding  $Z_4$   $\mathcal{N}$  families (Chapter 3), by using relations 6.3.1 and 6.3.2. The weight and  $\mathbb{N}$  distributions of  $\mathcal{N}^{LP}$ - $\mathcal{N}$  families are given in Table 6.4.1, Table 6.4.2 and Table 6.4.3.

Table 6.3.2. Correlation Distribution of  $\mathcal{N}^{LP}$ - $\mathcal{N}$  Family

a. Period: $2^r-1$ , $r$ an Odd Integer; $r=2t+1$		
Sl.No	$\mathbb{N}$	No of Occurrences
1	$2^r-1$	$2^r+1$ .
2.	$-1$	$(2^{2t}+1)(4^r-2)$ .
3.	$2^{t+1}-1$	$2^{t-1}(2^t+1)(4^r-2)$ .
4.	$-(2^{t+1}+1)$	$2^{t-1}(2^t-1)(4^r-2)$ .
b. Period: $2^r-1$ , $r$ an Even Integer, $r=2t$		
Sl.No	$\mathbb{N}$	No of Occurrences
1.	$2^r-1$	$2^r+1$ .
2.	$-1$	$3(2^{4t-3})(2^r+1)+(4^r-2)$ .
3.	$2^{t+1}-1$	$2^{3t-3}(2^{t-1}+1)(2^r+1)$ .
4.	$-(2^{t+1}+1)$	$2^{3t-3}(2^{t-1}-1)(2^r+1)$ .
5.	$2^t-1$	$2^{t-1}(2^t+1)(2^{2r-1}-2^{r-1}-2)$ .
6.	$-(2^t+1)$	$2^{t-1}(2^t-1)(2^{2r-1}-2^{r-1}-1)$ .

Table 6.4.1 Weight and Correlation Transform Distributions of  
 $\mathcal{NLS}\text{-}\mathcal{NM}(\text{tr}(\tilde{\gamma})=1)$  Families

a. Period  $2(2^r-1)$ ,  $r$  an Odd Integer;  $r=2t+1$

Sl. No.	$w_0$	$w_2$	Imbalance ( $w_0-w_2$ )	No of sequences
1.	$2^r+2^t-2$	$2^r-2^t$	$2^{t+1}-2$	$2^{t-1}(2^t+1)$
2.	$2^r-2^t-2$	$2^r+2^t$	$-(2^{t+1}+2)$	$2^{t-1}(2^t-1)$
3.	$2^r-2$	$2^r$	$-2$	1

b. Period  $2(2^r-1)$ ,  $r$  an Even Integer;  $r=2t$

Sl. No.	$w_0$	$w_2$	Imbalance ( $w_0-w_2$ )	No of sequences
1.	$2^r+2^t-2$	$2^r-2^t$	$2^{t+1}-2$	$2^{t-2}(2^{t-1}+1)$
2.	$2^r-2^t-2$	$2^r+2^t$	$-(2^{t+1}+2)$	$2^{t-2}(2^{t-1}-1)$
3.	$2^r-2$	$2^r$	$-2$	$2^{r-2}+1$

Table 6.4.2 Weight and Correlation Transform Distributions of  
 $\mathcal{NLS}\text{-}\mathcal{NM}(\text{tr}(\tilde{\gamma})=0)$  Families

a. Period  $2(2^r-1)$ ,  $r$  an Odd Integer;  $r=2t+1$

Sl. No.	$w_0$	$w_2$	Imbalance ( $w_0-w_2$ )	No of sequences
1.	$2^r+2^{t+1}-2$	$2^r-2^{t+1}$	$2^{t+2}-2$	$2^{t-2}(2^{t-1}+1)$
2.	$2^r-2^{t+1}-2$	$2^r+2^{t+1}$	$-(2^{t+2}+2)$	$2^{t-2}(2^{t-1}-1)$
3.	$2^r-2$	$2^r$	$-2$	$3(2^{2t-2})+1$

Table 6.4.2 Contined.

b. Period  $2(2^r-1)$ ,  $r$  an Even Integer;  $r = 2t$

Sl. No.	$w_0$	$w_2$	Imbalance ( $w_0-w_2$ )	No of sequences
1.	$2^r+2^t-2$	$2^r-2^t$	$2^{t+1}-2$	$2^{t-2}(2^{t-1}+1)$
2.	$2^r-2^t-2$	$2^r+2^t$	$-(2^{t+1}+2)$	$2^{t-2}(2^{t-1}-1)$
3.	$2^r-2$	$2^r$	$-2$	$2^{r-2}+1$

Table 6.4.3 Weight and Correlation Transform Distributions  
of  $\mathcal{NLP}\mathcal{NM}(\gamma=3)$  Families

a. Period  $2^r-1$ ,  $r$  an Odd Integer;  $r = 2t+1$

Sl. No.	$w_0$	$w_2$	Imbalance ( $w_0-w_2$ )	No of sequences
1.	$2^r+2^t-2$	$2^r-2^t$	$2^{t+1}-2$	$2^{t-1}(2^t+1)$
2.	$2^r-2^t-2$	$2^r+2^t$	$-(2^{t+1}+2)$	$2^{t-1}(2^t-1)$
3.	$2^r-2$	$2^r$	$-2$	1

b. Period  $2^r-1$ ,  $r$  an Even Integer,  $r = 2t$

Sl. No.	$w_0$	$w_2$	Imbalance ( $w_0-w_2$ )	No of sequences
1.	$2^r+2^t-2$	$2^r-2^t$	$2^{t+1}-2$	$2^{t-2}(2^{t-1}+1)$
2.	$2^r-2^t-2$	$2^r+2^t$	$-(2^{t+1}+2)$	$2^{t-2}(2^{t-1}-1)$
3.	$2^r-2$	$2^r$	$-2$	$2^{r-2}+1$

### 6.4.2 Correlation Distribution of $\mathcal{NLP}\text{-}\mathcal{IM}$ Families

From the linearity property and Lemma 6.2.1, the computation of correlation distributions runs on the same lines as given in Section 6.3.2, except that, here the number of sequences in a family is  $2^{r-1}+1$  and the period of sequences is  $2(2^r-1)$ . The computation is illustrated for the case of  $\mathcal{NLP}\text{-}\mathcal{IM}^{\gamma}(\text{tr}(\tilde{\gamma})=1)$ .

Correlation distribution  $\mathcal{D}$  of  $\mathcal{NLP}\text{-}\mathcal{IM}$  family is a set of crosscorrelation values of all pairs of sequences in the family; it is given by:

$$\mathcal{D} = \{C_{XY}(\tau), \text{ for all } X, Y \in \mathcal{NLP}\text{-}\mathcal{IM}, 0 \leq \tau \leq L, L:\text{period}\} \quad (6.3.4)$$

$$\mathcal{D} = \{C_{\varphi(\text{IS}^a), \varphi(\text{IS}^b)}(\tau), \text{IS}^a, \text{IS}^b \in \mathcal{NLP}\text{-}\mathcal{IM}, 0 \leq \tau \leq L, L:\text{period}\}.$$

Computations of correlation values in  $\mathcal{D}$  runs similar to computation for  $\mathcal{D}$  for  $\mathcal{NLP}\text{-}\mathcal{M}$  family (Section 6.3.2). Essentially, even in this case, it is sufficient to compute the correlation values of the following set  $\mathcal{D}'$ , given by

$$\begin{aligned} \mathcal{D}' = & \{\text{Re}(\Re(\text{IS}^{c\beta})) - \text{Im}(\Re(\text{IS}^{dc\beta}))\}; \text{ for all } c \text{ \& } \beta, c \in G_a, \beta \in G_c\} \\ & \cup \{\text{Re}(\Re(\text{IS}^{2\beta})) - \text{Im}(\Re(\text{IS}^{2(\beta+1)}))\}; \text{ for all } \beta, \beta \in G_c\} \cup \{2(2^r-1)\} \end{aligned} \quad (6.4.1)$$

where  $d = (1+2\beta^{-1})$ . Using arguments similar to the computation of  $\mathcal{D}$  for  $\mathcal{NLP}\text{-}\mathcal{M}$  family (Section 6.3),  $\mathcal{D}$  can be written as

$$\mathcal{D} = \{\mathcal{D}'\}^{2^{r-1}+1} \setminus \{\Re \text{ values of } \mathcal{NLP}\text{-}\mathcal{IM} \text{ family}\} \quad (6.4.2)$$

where  $\setminus$  represents set theoretic subtraction and superscripts indicate multiplicities. The 2<sup>nd</sup> set of  $\mathcal{D}'$ , takes a correlation value of  $-2$ ,  $2^r-1$  times, since  $\text{Im}(\Re(S^{2(\beta+1)})) = 0$ . Mainly it remains now only to compute the values in the first set. Here also, as  $\beta$  varies over  $G_c$ ,  $dc$  takes all values of  $G_a$  except  $c$ . The sample computation is illustrated below for  $\mathcal{NLP}\text{-}\mathcal{IM}^{\gamma}(\text{tr}(\tilde{\gamma})=1)(r : \text{odd})$ . The exact values of  $\Re$  of  $\text{Im}$ -sequences  $\text{IS}^a$  for all  $a \in G_a/(1, \gamma)$  (the values in the subsets  $\mathcal{P}$ ,  $\mathcal{Q}$ ,  $\mathcal{R}$ , and  $\mathcal{S}$ ) are given Tables 3.5.1, 3.5.2 and 3.5.3. But, we need  $\Re$  values of all  $\text{IS}^a$ ,  $a \in G_a$ . Since  $\Re(\text{IS}^a) = \Re(\text{IS}^{a\gamma})$ ,  $\Re$  values of  $\mathcal{P}$ ,  $\mathcal{Q}$ ,  $\mathcal{R}$ , and  $\mathcal{S}$  appear twice in the set  $\{\Re(\text{IS}^a), a \in G_a\}$ . Thus, the distribution  $\Re$  values in  $\{\Re(\text{IS}^a), a \in G_a\}$  is obtained from  $\Re$  distribution of  $\mathcal{IM}$  family by multiplying a value of 2 to 'no of occurrences' column of the entries corresponding to  $\mathcal{P}$ ,  $\mathcal{Q}$ ,  $\mathcal{R}$ , and  $\mathcal{S}$ . The distribution of  $\{\Re(\text{IS}^a), a \in G_a\}$  for  $\mathcal{NLP}\text{-}\mathcal{IM}^{\gamma}(\text{tr}(\tilde{\gamma})=1)(r : \text{odd})$  family, is given by

Sl.No	Subset	$\aleph$	No of Occurences
1.	$\overline{\mathcal{P}}$	$2(2^t-1)$	$2^t(2^{t-1}+1)$
2.	$\overline{\mathcal{Z}}$	$-2(2^t+1)$	$2^t(2^{t-1}-1)$
3.	$\overline{\mathcal{R}}$	$-2 + \omega 2^{t+1}$	$2^{2t-1}$
4.	$\overline{\mathcal{S}}$	$-2 - \omega 2^{t+1}$	$2^{2t-1}$

Refer the  $\aleph$  values above, when  $c \in \overline{\mathcal{P}}$ ,  $\aleph(\text{IS}^c) = 2(2^t-1)$  and as  $\beta$  varies over all  $G_c$ ,  $\text{IS}^{\text{dc}}$  takes all the sequences from subsets  $\overline{\mathcal{P}}$ ,  $\overline{\mathcal{Z}}$ ,  $\overline{\mathcal{R}}$ ,  $\overline{\mathcal{S}}$  except  $\text{IS}^c$  it self. Hence the correlation value of

$$\text{Re}(\aleph(\overline{\mathcal{P}})) - \text{Im}(\aleph(\overline{\mathcal{P}})) = 2(2^t-1) \text{ appears } |\overline{\mathcal{P}}|(|\overline{\mathcal{P}}|-1) = (2^t(2^{t-1}+1))(2^t(2^{t-1}+1)-1) \text{ times,}$$

$$\text{Re}(\aleph(\overline{\mathcal{P}})) - \text{Im}(\aleph(\overline{\mathcal{Z}})) = 2(2^t-1) \text{ appears } |\overline{\mathcal{P}}||\overline{\mathcal{Z}}| = (2^t(2^{t-1}+1))(2^t(2^{t-1}-1)) \text{ times,}$$

$$\text{Re}(\aleph(\overline{\mathcal{P}})) - \text{Im}(\aleph(\overline{\mathcal{R}})) = -2 \text{ appears } |\overline{\mathcal{P}}||\overline{\mathcal{R}}| = (2^t(2^{t-1}+1))2^{2t-1} \text{ times,}$$

$$\text{Re}(\aleph(\overline{\mathcal{P}})) - \text{Im}(\aleph(\overline{\mathcal{S}})) = 2^{t+2}-2 \text{ appears } |\overline{\mathcal{P}}||\overline{\mathcal{S}}| = (2^t(2^{t-1}+1))2^{2t-1} \text{ times.}$$

Similarly the correlation values are computed for  $c \in \overline{\mathcal{Z}}$ ,  $\overline{\mathcal{R}}$  and  $\overline{\mathcal{S}}$ . This way the correlation distribution  $\mathcal{D}$  is computed. Similarly correlation distribution of other  $\mathcal{NLP}$  families are computed and distributions are given in Tables 6.4.4, 6.4.5, and 6.4.6.

Table 6.4.4 Crosscorrelation Distribution of  $\mathcal{N}_{2^r-1}(\text{tr}(\gamma)=1)$  Familya. Period  $2(2^r-1)$ ,  $r$  an Odd Integer;  $r = 2t+1$ 

Sl.No	$\kappa$	No of Occurrences
1.	$2(2^r-1)$	$2^{r-1}+1$
2.	$(2^{t+1}-2)$	$2^{t-1}(2^t+1)(2^{2r-1}-3)$
3.	$-(2^{t+1}+2)$	$2^{t-1}(2^t-1)(2^{2r-1}-3)$
4.	$(2^{t+2}-2)$	$2^t(2^{t-1}+1)(2^{r-1}+1)2^{r-2}$
5.	$-(2^{t+2}+2)$	$2^t(2^{t-1}-1)(2^{r-1}+1)2^{r-2}$
6.	$-2$	$3(2^{3r-4}+2^{2r-3}) + (2^{2r-1}+2^{r-1}-2)$

b. Period  $2(2^r-1)$ ,  $r$  an Even Integer,  $r = 2t$ 

Sl.No	$\kappa$	No of Occurrences
1.	$2(2^r-1)$	$(2^{r-1}+1)$
2.	$(2^{t+1}-2)$	$2^{t-2}(2^{t-1}+1)(2^{2r}+2^r-3)$
3.	$-(2^{t+1}+2)$	$2^{t-2}(2^{t-1}-1)(2^{2r}+2^r-3)$
4.	$-2$	$2^{2t-2}(2^{2r}+2^r-3) + (2^{2r-1}+2^{r-1}-2)$

Table 6.4.5. Correlation Distribution of  $\mathcal{N}\mathcal{L}\mathcal{P}\text{-}\mathcal{N}\mathcal{M}(\text{tr}(\gamma)=0)$  Familya. Period  $2(2^r-1)$ ,  $r$  an Odd Integer;  $r = 2t+1$ 

Sl.No	$\chi$	No of Occurrences
1.	$2(2^r-1)$	$(2^{r-1}+1)$
2.	$(2^{t+1}-2)$	$2^{4t}+2^{3t}(2^{r-1}+1)$
3.	$-(2^{t+1}+2)$	$2^{4t}-2^{3t}(2^{r-1}+1)$
4.	$(2^{t+2}-2)$	$2^{t-2}(2^{t-1}+1)(2^{2r-1}-3)$
5.	$-(2^{t+2}+2)$	$2^{t-2}(2^{t-1}-1)(2^{2r-1}-3)$
6.	$-2$	$3(2^{r-2})(2^{2r-1}-3) + (2^{2r-1}+2^{r-1}-2)$

b. Period  $2(2^r-1)$ ,  $r$  an Even Integer,  $r = 2t$ 

Sl.No	$\chi$	No of Occurrences
1.	$2(2^r-1)$	$(2^{r-1}+1)$
2.	$(2^{t+1}-2)$	$2^{t-2}(2^{t-1}+1)(3 \cdot 2^{2r-2}+2^{r-1}-3)$
3.	$-(2^{t+1}+2)$	$2^{t-2}(2^{t-1}-1)(3 \cdot 2^{2r-2}+2^{r-1}-3)$
4.	$(2^{t+2}-2)$	$2^{t-1}(2^{t-2}+1)(2^{2r-4}+2^{r-3})$
5.	$-(2^{t+2}+2)$	$2^{t-1}(2^{t-2}-1)(2^{2r-4}+2^{r-3})$
6.	$-2$	$2^{r-2}(19 \cdot 2^{2r-4}+11 \cdot 2^{r-3}-3) + (2^{2r-1}+2^{r-1}-2).$

Table 6.4.6 Correlation Distribution of  $\mathcal{NL}^2\text{-}\mathcal{NL}^3$  Family

a. Period $2(2^r-1)$ , $r$ an Odd Integer; $r = 2t+1$		
Sl.No	$\lambda$	No of Occurrences
1.	$2(2^r-1)$	$2^{r-1}+1$
2.	$2(2^t-1)$	$2^{t-1}(2^t+1)(2^{2r}+2^r-3)$
3.	$-2(2^t+1)$	$2^{t-1}(2^t-1)(2^{2r}+2^r-3)$
4	$-2$	$(2^{2r-1}+2^{r-1}-2)$
b. Period $2(2^r-1)$ , $r$ an Even Integer, $r = 2t$		
Sl.No.	$\lambda$	No of Occurrences
1.	$2(2^r-1)$	$(2^{r-1}+1)$
2.	$(2^{t+1}-2)$	$2^{t-2}(2^{t-1}+1)(2^{2r}+2^r-3)$
3.	$-(2^{t+1}+2)$	$2^{t-2}(2^{t-1}-1)(2^{2r}+2^r-3)$
4.	$-2$	$2^{r-2}(2^{2r}+2^r-3) + (2^{2r-1}+2^{r-1}-2)$

## 6.5. Linear Complexity Computation of $\mathcal{NL}^2$ Sequences

This section gives the LC distribution of  $\mathcal{NL}^2$  sequences.  $\mathcal{NL}^2$  sequences are defined over the ideal  $\langle 2 \rangle \in \mathbb{Z}_4$  which is isomorphic to binary field. The LC of  $\mathcal{NL}^2$  sequences is computed using generalized Blahut's theorem (Theorem 2.5.3) for computing LC of sequences over  $\mathbb{Z}_4$ . Since the ideal  $\langle 2 \rangle$  is isomorphic to  $\text{GF}(2)$ , LC thus computed over ideal sequences are indeed LC of binary sequences. Using Theorem 2.5.5, the LC of  $\{s_i\}$  of period  $2^r-1$  can be determined by expanding  $s_i$  in the form

$$s_i = \sum_{j=0}^{2^r-1} s_j \alpha^{ji}, i \in \mathbb{Z}_{2^r-1} \quad (6.5.1)$$

where  $\alpha$  is primitive in  $\mathbb{G}_c$  and counting number of non zero coefficients in the expansion.

$$\text{LC}(\{s_i\}) = |\{ \tilde{s}_j : \tilde{s}_j \neq 0, 0 \leq j < 2^r-1 \}| \quad (6.5.2)$$



The representation of (6.5.1) is unique since  $2^r-1$  is relatively prime to 4, which is the characteristic of the ring  $Z_4$  and  $\tilde{s}_j$ 's in (6.5.1) is given by

$$\tilde{s}_j = \sum_{i=0}^{2^r-2} s_i \alpha^{-ji}, j \in Z_{2^r-1} \quad (6.5.3)$$

$\tilde{s}_j$ 's are fourier transform coefficients of the sequence S.

Theorem 6.5.1 gives the LC of  $\mathcal{NLPS}$  sequences.

**Theorem 6.5.1:** The LC of a zeroth level  $\mathcal{NLPS}$  sequences of period  $2^r-1$  is either  $r(r+1)/2$  and  $r(r-1)/2$ . First level  $\mathcal{NLPS}$  sequence is a binary m-sequence and LC is r.

**Proof:** A  $\mathcal{NLPS}$  sequence corresponding to m-sequence  $S^a$  is given by

$$S = \{s_i\} = \varphi(S^a); s_i = \varphi(\text{tr}_1^r(a\alpha^i)), i \in Z_{2^r-1}$$

Expanding the above equation using the definition of trace function we get

$$s_i = \sum_{j=0}^{r-1} \alpha^{(2^j)^i} (1 - \sigma^{j-1}(a)) + 2 \sum_{j_1=0}^{r-2} \sum_{j_2=j_1+1}^{r-1} \sigma^{j_1}(a) \sigma^{j_2}(a) \alpha^{(2^{j_1}+2^{j_2})i}$$

It is easy to verify that  $2^{j_1}+2^{j_2}$ ,  $0 \leq j_1 \leq r-2$ ,  $j_1 < j_2 < r$ , is always less than  $2^r-1$ , and all are distinct integers which are not powers of 2. Hence, second term contributes LC of  $r(r-1)/2$ . First term will be non zero if  $a \neq 1$ . Hence LC of  $\varphi_1(S^a)$  is  $r(r-1)/2 + r = r(r+1)/2$  for all  $a \in G_a$ , except  $a = 1$ . For  $a = 1$ , LC of  $\varphi_1(S^1)$  is  $r(r-1)/2$ .  $\square$

In case of  $\mathcal{NLPS}$  Im-sequences we cannot make use of Blahut's theorem since the period of Im-sequences is  $2(2^r-1)$  and the representation of (6.5.1) is not valid. In this case the roots of characteristic polynomial of sequences divides polynomial  $(x^{2^r-1}-1)^2$  and hence the multiplicity of roots can be at the maximum 2. The LC of the first level sequence which is a binary m-sequence is r like in  $\mathcal{NLPS}$ . Theorem 6.5.2 gives LC of zeroth level  $\mathcal{NLPS}$ Im-sequences.

**Theorem 6.5.2:** The LC of a zeroth level  $\mathcal{NLPS}$ Im sequences of period  $2(2^r-1)$  is equal to  $r(r+3)/2$ .

**Proof:** A zeroth level  $\mathcal{NLPS}$  sequence, corresponding to an Im-sequence  $IS^a$  is given by

$$S = \{s_i\} = \varphi(IS^a); s_i = \varphi(\text{tr}_1^r(a(\gamma\alpha)^i)), i \in Z_{2(2^r-1)}$$

Expanding the above equation we get  $s_i = s_i' + s_i''$ , where

$$\begin{aligned}
s_i' &= 2 \sum_{j_1=0}^{r-2} \sum_{j_2=j_1+1}^{r-1} \sigma^{j_1}(a) \sigma^{j_2}(a) \alpha^{(2^{j_1}+2^{j_2})i} \\
&= 2 \sum_{j_1=0}^{r-2} \sum_{j_2=j_1+1}^{r-1} \alpha^{(2^{j_1}+2^{j_2})i}, \text{ since } 2b = 1 \text{ for } b \in G_a; \text{ and} \\
s_i'' &= \sum_{j=0}^{r-1} \alpha^{(2^j)i} (1 - \sigma^{j-1}(a) \sigma^{j-1}(\gamma)) \\
&= 2 \sum_{j=0}^{r-1} \alpha^{(2^j)i} P_j(i),
\end{aligned}$$

where  $P_j(i)$  is polynomial in  $i$  of degree 1, and is given by  $P_j(i) = (\sigma^{j-1}(\bar{a}) + i^* \sigma^{j-1}(\bar{\gamma}))$ ,  $a = 1 + 2(\bar{a})$ . Then from Theorem 6.21 [67],  $\{s_i''\}$  is the solution of linear recursion with characteristic polynomial having roots  $\alpha^{2^i}$ ,  $i = 0, \dots, r-1$ , with multiplicity two. Hence LC of  $\{s_i''\}$  is  $2r$ . Sequence  $\{s_i'\}$  as in the previous case, has roots  $\alpha^{(2^{j_1}+2^{j_2})i}$ ,  $0 \leq j_1 \leq r-1$ ,  $j_1 < j_2 \leq r-1$ , in its representation which does not coincide with  $\alpha^{2^i}$ ,  $i=0, \dots, r-1$ . Hence the LC of  $\{s_i\}$  is given by  $2r+r(r-1)/2 = r(r+3)/2$ . Unlike  $\mathcal{NLP}$ - $\mathcal{M}$  sequences, all  $\mathcal{NLP}$ -I-m-sequences have LC of  $r(r+3)/2$ . The LC of distributions  $\mathcal{NLP}$  families are given in the following table.

Table 6.5.1 Linear Complexity Distribution of  $\mathcal{NLP}$  Sequences

$\mathcal{NLP}$ - $\mathcal{M}$ family			$\mathcal{NLP}$ - $\mathcal{IM}$ families	
LC	No of Sequences	Group	No of Sequences	Group
$r$	1	m-sequence	1	m-sequence
$r(r-1)/2$	1	$\varphi(S^1)$	0	
$r(r+1)/2$	$2^r-1$	$\varphi(S^a)$ , $a \neq 1 \in G_a$	0	
$r(r+3)/2$	0		$2^{r-1}$	$\varphi(S^a)$ $a \in G_a/\{1, \gamma\}$

*Example 6.5.1:* Sequences of  $\mathcal{NLP}\text{-}\mathcal{M}$   $\mathcal{NLP}$  sequences over  $\langle 2 \rangle$  derived from m-sequences of period  $L = 7$  generated by  $\alpha \in G_c$  of  $GR^*(4,3)$ , such that  $1+3\alpha+2\alpha^2=\alpha^3$ , are given in Table 6.5.2.

*Example 6.5.2:* Sequences of  $\mathcal{NLP}\text{-}\mathcal{M}$  Sequences of  $\mathcal{NLP}\text{-}\mathcal{M}$  of period 15:  $\mathcal{NLP}$  sequences over  $\langle 2 \rangle$  derived from m-sequences of period  $L = 15$  generated by  $\alpha \in G_c$  of  $GR^*(4,4)$ , such that  $3+\alpha+2\alpha^2=\alpha^4$ , are given in Table 6.5.3. The minimum polynomial  $m_\alpha(d)$  is  $(1+3d+2d^2+d^4)$ .

*Example 6.5.3:*  $\mathcal{NLP}$  families of sequences derived from Im-sequences of period 30; three representative examples of different types of  $\mathcal{NLP}\text{-}\mathcal{M}$  families are given in Table 6.5.4.

*Example 6.5.4:*  $\mathcal{NLP}$  families of sequences derived from Im-sequences of period 62; three representative examples of different types of  $\mathcal{NLP}\text{-}\mathcal{M}$  families are given in Table 6.5.5. In Tables 6.5.2 – 6.5.5, Galois ring elements are represented as vectors over  $Z_4$  within brackets.

Table 6.5.2 Sequences of  $\mathcal{NLP}\text{-}\mathcal{M}$  of Period 7 (Example 6.5.1)

(a)	Sequence S	Imbalance	LC
(100)	2 2 2 2 2 2 0	-5	6
(300)	2 2 0 2 0 0 2	-1	3
(120)	2 0 2 0 0 0 0	3	6
(320)	2 0 0 0 2 2 2	-1	6
(102)	0 2 0 0 0 2 0	3	6
(302)	0 2 2 0 2 0 2	-1	6
(122)	0 0 0 2 2 0 0	3	6
(322)	0 0 2 2 0 2 2	-1	6
(100)	0 0 2 0 2 2 2	-1	3

Table 6.5.3 Sequences of  $\mathcal{N}^{\mathcal{A}}\mathcal{N}$  of Period 15 (Example 6.5.2)

(a)	Sequence S	Imbalance	LC
(1000)	000020200220220	3	10
(3000)	002022002202000	3	6
(1200)	020002220002020	3	10
(3200)	022000022020200	3	10
(1020)	200200002002220	3	10
(3020)	202202200020000	3	10
(1220)	220222022220020	-5	10
(3220)	222220220202200	-5	10
(1002)	002222222000222	-5	10
(3002)	000220020022002	3	10
(1202)	022200202222022	-5	10
(3202)	020202000200202	3	10
(1022)	202002020222222	-5	10
(3022)	200000222200002	3	10
(1222)	222020000000022	3	10
(3222)	220022202022202	-5	10
(1000)	002002202022220	-1	4

Table 6.5.4  $\mathcal{NLP}$  Families of Im-sequences of Period 30 (Example 6.5.3)a. Sequences of Family  $\mathcal{NLP}\text{-}\mathcal{N}(\text{tr}(\tilde{\gamma}) = 1; \gamma = (1002)$ Sequences are generated by  $\gamma\alpha$ ,  $\gamma = (1002)$ ,  $\alpha = (0100)$ ,  $\gamma\alpha = (2300)$ Minimal polynomial corresponding to  $\gamma\alpha$  is  $3+d+2d^2+d^4$ 

LC of sequences = 14

a	Sequence	Imbalance)
(1000)	00202020220022200022220020220	-2
(3000)	000022000222002002220022002000	6
(1200)	02200222202022020200200202020	-2
(3200)	020000020000202022202002220200	6
(1020)	2022000000222220000202202220	-2
(3020)	200202202000002202000220220000	6
(1220)	22222020200022220020002020020	-2
(3220)	220202222220222202200002200	-10
(1000)	00200220202220002002202022220	-2

b. Sequences of Family  $\mathcal{NLP}\text{-}\mathcal{N}(\text{tr}(\tilde{\gamma}) = 0; \gamma = (1200)$ Sequences are generated by  $\gamma\alpha$ ,  $\gamma = (1200)$ ,  $\alpha = (0100)$ ,  $\gamma\alpha = (0120)$ Minimal polynomial corresponding to  $\gamma\alpha$  is  $1+3d+d^4$ 

LC of sequences = 14

a	Sequence	$\aleph(\text{IS}^a)$
(1000)	00000020020002002002220022220	6
(3000)	002002002222200022020022000000	6
(1020)	2002200020220202202022200220	-2
(3020)	202222200000200222200220222000	-2
(1002)	0022022220200220222202202222	-10
(3002)	0002000200022020222000220002	6
(1022)	2020220202022222000000020222	-2
(3022)	20002022220202220002202002002	-2
(1000)	00200220202220002002202022220	-2

Table 6.5.4 Continued..

c. Sequences of Family  $\mathcal{NL}\mathcal{P}\text{-}\mathcal{JM}'(\gamma = 3)$ Sequences are generated by  $\gamma\alpha$ ,  $\gamma = (3000)$ ,  $\alpha = (0100)$ ,  $\gamma\alpha = (0300)$ Minimal polynomial corresponding to  $\gamma\alpha$  is  $1+d+2d^2+d^4$   
LC of sequences = 14

a	Sequence	Imbalance
(1000)	002020002200020000022200222200	6
(1200)	022002022022220020000220000000	6
(1020)	202200200022020200202002000200	6
(1220)	22222220200220220220022222000	-10
(1002)	000222020020022002220222002202	-2
(1202)	02020000020222202202202220002	-2
(1022)	20000222202022202000020220202	-2
(1222)	220020202022222022000002002	-2
(1000)	00200220202222000200220202220	-2

Table 6.5.5  $\mathcal{NL}\mathcal{P}\text{-}\mathcal{JM}$  Families of Period 62 (Example 6.5.4)a. Sequences of Family  $\mathcal{NL}\mathcal{P}\text{-}\mathcal{JM}'(\text{tr}(\gamma) = 1; \gamma = (32000))$ 

LC of sequences = 20

Sequences are generated by  $\gamma\alpha$ ,  $\gamma = (32000)$ ,  $\alpha = (01000)$ ,  $\gamma\alpha = (03200)$ Minimal polynomial corresponding to  $\gamma\alpha$  is  $1+d^2+2d^3+d^5$ .

a	IS <sup>a</sup>	K(IS <sup>a</sup> )
(10000)	00202020220022200202000002222002022222200022200220222222202	-10
(12000)	02220022002222222202020202220000000220002202202000220222222	-10
(10200)	20022002002022020020020020202220220220000200200020000202222002	6
(12200)	22000000220222002002222220220002022022220202222220000222022	-10
(10020)	0200220200002000202220200020222002220000000002220222022220200	6
(12020)	000202002222200200000000202020220000222220000022002220220220	6
(10220)	2222222022202222200222200222000202222200020202020002220000	-10
(12220)	202002220002202002220220200022202002000020022000200220020020	6
(10002)	222002020200002220000200000220020020000020020222000222202222	6
(12002)	202222002202002000222220200222022002202220220220220020202202	-10
(10202)	020220202020000022220002000200000200022202020022002202202022	6
(12202)	000022220202000202002220020200222020022000002022000202002	6
(10022)	20000020200002020220220000022222000220000002002220022200200	6
(12022)	2202202202220202020200200022220220222022022022022002200200	-10
(10222)	00220002200222000022022022000002020002000222202222002200020	6
(12222)	02202000200222202000022000022002220220220220002200200000	6
(10000)	0020220022222000220222020200002002220222200022022020200002	-2

Table 6.5.5 Continued..

b. Sequences of Family  $\mathcal{NLS}\text{-}\mathcal{NM}'(\text{tr}(\tilde{\gamma}) = 0; \gamma = (12000))$ Sequences are generated by  $\gamma\alpha$ ,  $\gamma = (12000)$ ,  $\alpha = (01000)$ ,  $\gamma\alpha = (01200)$ Minimal polynomial corresponding to  $\gamma\alpha$  is  $3+3d^2+2d^3+d^5$ 

LC of sequences = 20

a	IS <sup>a</sup>	$\kappa(\text{IS}^a)$
(10000)	00000020022002202202200000222220202220022022022000202022202	-2
(30000)	0020222020022220000002020222200220222022022202222222222200	-18
(10200)	20220002200002022020220002202222020000222020000020222202002	-2
(30200)	20022202022220222020000022202200002002200000202222020022000	-2
(10020)	0220020220200000002200200020220002222000202000220002000202020	14
(30020)	0200200202200002220222202220002000020200202020202022220202	-2
(10220)	2202022002000022020002220020020200022220220020222220220000	-2
(30220)	22222020222022202200220200220022202002200020000200002220002	-2
(10002)	220022022220220200002200000220220020200002202020220202002222	-2
(30002)	2220000200020022220200020202200202200022200020022020222202220	-2
(10202)	02222200000200002222002000200200200222222200222000022200222	-2
(30202)	020200202220000202002000202000000020220000002000222202202020	14
(10022)	20202020002022022200220000020022220022202200020222002000220	-2
(30022)	20000220220202020022202202002022202220020020020000022200222	-2
(10222)	0002200222002202002002200000002000000022222002020022000020	14
(30222)	00220202002202200200222020002022200220002222220202200200022	-2
(10000)	002022002222200020222020200002002022002222000220222020200002	-2

c. Sequences of Family  $\mathcal{NLS}\text{-}\mathcal{NM}'(\gamma = 3)$ Sequences are generated by  $\gamma\alpha$ ,  $\gamma = (30000)$ ,  $\alpha = (01000)$ ,  $\gamma\alpha = (03000)$ Minimal polynomial corresponding to  $\gamma\alpha$  is  $1+2d+d^2+d^5$ 

LC of sequences = 20

a	IS <sup>a</sup>	$\kappa(\text{IS}^a)$
(10000)	0020002002202220222202022220000022202002022000200222222222	-10
(12000)	02222022200222220200000002220002020222022002222002220222202	-10
(10200)	2002000220002202200022222022020222202022020202020020222022	-10
(12200)	2200200002222000022020200220002220020020000200222020000222002	6
(10020)	02000202202020000002000020222022020202020000220022022220220	6
(12020)	000222000202200220202020002020200220000202000020222202202020	6
(10220)	22220220020020220220022202202022022022022002222000222002	-10
(12220)	2020222202220220222200200022000002202000200000020022220022202	6
(10002)	222022022220002200202220220220022000020002202222200222202202	-10
(12002)	202202000002002020020200000222020022000222020200200200202222	6
(10202)	02022220000000000202222002000022200202222000200002202202002	6
(12202)	00000222222000222200002000202000202200002002002222000202022	6
(10022)	20002020002002022200020020002022020022202202000220022200200	6
(12022)	220200222202020002222200000222222200202200202000220200220	-10
(10222)	0022200222000220202200022000020002020022220022220220020000	6
(12222)	022000000220222000022000020002020022222022022220220200200020	6
(10000)	002022002222200020222020200002002022002222000220222020200002	-2

## 6.6 Comparison of New Biphase Constructions with Known Families

Table 6.6.1 gives the comparison of binary families derived in this paper with previously known constructions. Many new optimal families are added to the list. The family  $\mathcal{NLP}\text{-}\mathcal{JN}(\gamma = 3)$  is interesting in the sense that it satisfies welch bound on  $\theta_{\max}$  ( $\theta_{\max} < \sqrt{L}$ ) and compares with bent and Kasami (small set) sequences. The number of sequences in the new family is  $L/4$ , where as Kasami and Bent sequences have only  $\sqrt{L}$  sequences in their family. However, unlike Kasami and Bent, new families are not balanced. With respect to LC, the performance of the new family is in between Kasami and Bent sequences. If the sequences with period  $2^r - 1$  of these families are compared, the LC's of Kasami sequences, bent sequences and the new families are linear in  $r$  ( $2r$ ), exponential in  $r$  and quadratic in  $r$  respectively. In the following table optimal Sidelnikov bound means  $\theta_{\max} \leq \sqrt{2L}$ , and suboptimal sidelnikov means  $\theta_{\max} \leq 2\sqrt{L}$ .

If we closely observe the correlation properties of  $\mathcal{NLP}$  sequence families, we note that not always optimal  $Z_4$  families (Welch bound) has resulted optimal binary families. In one case suboptimal  $Z_4$  sequence family has yielded an optimal binary sequence family. Table 6.6.2 gives the properties of various quadriphase and biphase sequence families obtained under  $\mathcal{NLP}$  mapping.



Table 6.6.1 Comparison of New Biphas Sequence Constructions with Previously Known Families

Family	Period N	Family size	Maximum achievable Linear span	$C_{\max}$	Comment
Gold	$2^r-1$ (r : odd)	$2^r+1$	$2r$	$1+2^{(r+1/2)}$	Optimal (Sidelnikov)
Gold	$2^r-1$ (r : even)	$2^r+1$	$2r$	$1+2^{(r+2/2)}$	Suboptimal (Sidelnikov)
Kasami Small set	$2^r-1$ (r : even)	$2^{r/2}$	$3r/2$	$1 + 2^{r/2}$	Optimal (Welch)
Kasami Large set	$2^r-1$ (r : even)	$2^{r/2}(2^r+1)$	$5r/2$	$1+2^{(r+2/2)}$	SubOptimal (Sidelnikov)
Bent Sequences	$2^r-1$ (r : 4t)	$2^{r/2}$	$\begin{bmatrix} r/2 \\ r/4 \end{bmatrix} 2^{r/4}$	$1 + 2^{r/2}$	Optimal (Welch)
$\mathcal{NLDP}-\mathcal{M}$	$2^r-1$ (r : odd)	$2^r+1$	$r(r+1)/2$	$1+2^{(r+1/2)}$	Optimal (Sidelnikov)
$\mathcal{NLDP}-\mathcal{M}$ (r : even)	$2^r-1$	$2^r+1$	$r(r+1)/2$	$1+2^{(r+1/2)}$	Suboptimal (Sidelnikov)
$\mathcal{NLDP}-\mathcal{JN}^{\gamma}$ $\text{tr}(\gamma)=0$ $\text{tr}(\gamma)=1$	$2(2^r-1)$ (r : odd)	$2^{r-1}+1$	$\geq r(r+3)/2$	$2(1+2^{(r+1/2)})$	Suboptimal (Sidelnikov)
$\mathcal{NLDP}-\mathcal{JN}^{\gamma}$ ( $\gamma=3$ )	$2(2^r-1)$ (r:odd)	$2^{r-1}+1$	$\geq r(r+3)/2$	$2(1+2^{(r-1/2)})$	Optimal (Welch)
$\mathcal{NLDP}-\mathcal{JN}^{\gamma}$ $\text{tr}(\gamma)=1$ ( $\gamma=3$ )	$2(2^r-1)$ (r:even)	$2^{r-1}+1$	$\geq r(r+3)/2$	$2(1+2^{(r/2)})$	Optimal (Sidelnikov)
$\mathcal{NLDP}-\mathcal{JN}^{\gamma}$ $\text{tr}(\gamma)=0$	$2(2^r-1)$ (r:even)	$2^{r-1}+1$	$\geq r(r+3)/2$	$2(1+2^{(r+1/2)})$	Suboptimal (Sidelnikov)

Table 6.6.2. Optimality Properties of Quadriphase and Biphas families under  $\mathcal{NLP}$  Mapping

Family	Period	Quadriphase family	bi-phase family
$\mathcal{K}$	$2^r-1$ ( $r$ : odd)	Optimal (Welch)	Optimal (Sidelnikov)
$\mathcal{K}$	$2^r-1$ ( $r$ : even)	Optimal (Welch)	Sub optimal (Sidelnikov)
$\mathcal{K}^{\gamma}(\text{tr}(\tilde{\gamma})=1)$	$2(2^r-1)$ ( $r$ : odd)	Optimal (Welch)	Sub optimal (Sidelnikov)
$\mathcal{K}^{\gamma}(\gamma=3)$	$2(2^r-1)$ ( $r$ : odd)	Optimal (Welch)	Optimal (Welch)
$\mathcal{K}^{\gamma}(\text{tr}(\tilde{\gamma})=0)$	$2(2^r-1)$ ( $r$ : odd)	Sub optimal (Welch)	Sub optimal (Sidelnikov)
$\mathcal{K}^{\gamma}(\text{tr}(\tilde{\gamma})=1)$	$2(2^r-1)$ ( $r$ : odd)	Optimal (Welch)	Optimal (Sidelnikov)
$\mathcal{K}^{\gamma}(\gamma=3)$	$2(2^r-1)$ ( $r$ : even)	Sub optimal (Welch)	Optimal (Sidelnikov)
$\mathcal{K}^{\gamma}(\text{tr}(\tilde{\gamma})=0)$ ( $r$ : even)	$2(2^r-1)$	Sub optimal (Welch)	Sub optimal (Sidelnikov)

## Chapter 7

### Sequences over Semi-local Residue Class Polynomial Rings

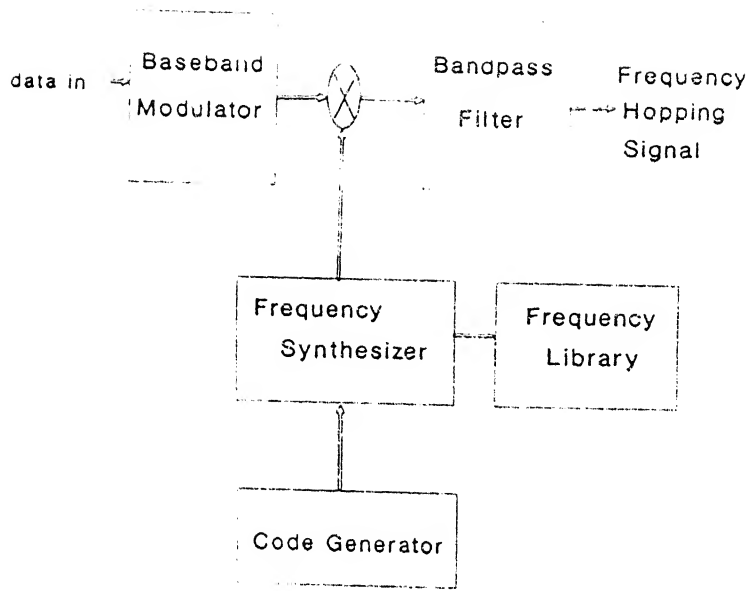
This chapter is concerned with construction of slow frequency hopping (SFH) patterns derived from sequences over semi-local rings  $P_p^n[w(\xi)]$ , where  $w(\xi)$  is a composite polynomial of degree  $n$  over  $GF(p)$ . Various families of frequency hopping patterns are constructed using internal direct sum representation of semi-local rings  $P_p^n[w(\xi)]$  and families of sequences over local rings  $P_p^{n_1}[w_1(\xi)^k]$ , where  $w_1(\xi)^k$  is a factor of  $w(\xi)$ . For convenience indeterminate  $\xi$  from the residue class polynomial ring symbol  $P_p^n[w(\xi)]$  may be dropped. Internal direct sum representation of  $P_p^n[w]$  is given in Appendix F. These families have nice generalized Hamming correlation properties (the generalized correlation function is given Section 1.2).

The chapter is organized as follows. Section 7.1 gives a brief description of slow hopping multiple-access (M-A) communication systems and requirements on the hopping patterns. Section 7.2 gives a construction of SFH patterns from sequences over orthogonal ideals of  $P_p^n[w]$ . Internal direct sum decomposition of the ring  $P_p^n[w]$  into orthogonal ideals is given Appendix F. Families of sequences with ideal generalized Hamming correlation properties are presented. Construction of SFH patterns derived from one-coincidence sequences over  $P_p^{n_1}[(w_1)^k]$ , where  $n_1 < n$  and  $(w_1)^k$  is a factor of  $w(\xi)$ , is given in Section 7.3. Section 7.4 gives a SFH pattern generation procedure where different users have different frequency expansion factors.

#### 7.1 Slow Frequency Hopping Multiple Access Communication Systems

Slow frequency hopping is one of the common techniques for spreading the signal spectrum in data communication. The amount of frequency spread is in far excess of the minimum bandwidth necessary to transmit the data (information bandwidth). This fact makes it feasible for many users to share a common channel. The channel is a simple OR channel; at every time instant it accepts  $n$  input signals  $X_1, X_2, \dots, X_n$  and emits  $X_1 \text{ OR } X_2 \text{ OR } \dots \text{ OR } X_n$  at its output. In such a M-A situation, the channel bandwidth must be greater than or equal to the sum of information bandwidths of individual users in the system.

The frequency library in a slow frequency hopping M-A system consists of large number of frequency carriers (frequency library of size  $|\mathcal{A}|$ ) which are chosen to be orthogonal to each other over the transmission time duration  $T$  (these carriers are obtained by subdividing the entire bandwidth into



a. Transmitter

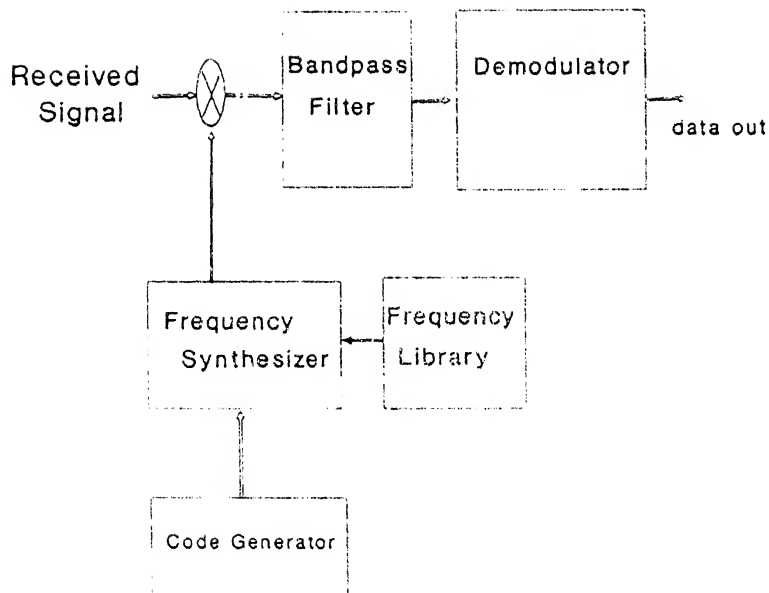


Fig 7.1.1 Slow Frequency Hopping Spread Spectrum System

b. Receiver.

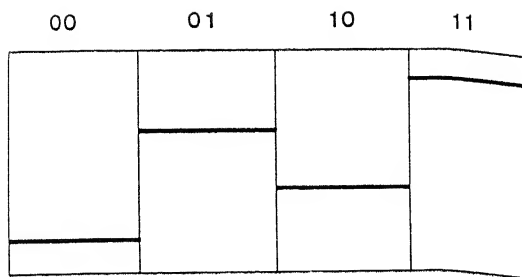


Fig 7.1.2 Time-frequency Graph of the Baseband Signal

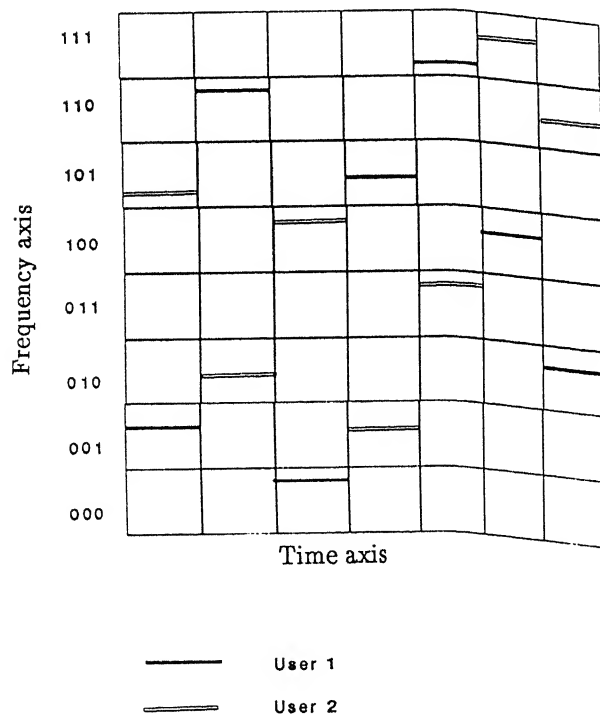


Fig 7.1.3 Time-frequency Graph of the Transmitted Signal for Example 7.1.1

### 7.1.1 Correlation Requirements on the Patterns

Normally, in frequency hopping systems, it is required that mutual Hamming correlation between sequences should be small. In SFH M-A communication systems, one or more symbols are transmitted within one frequency hop (slot) and a hit would mean total loss of data transmitted in that hop [93]. Thus, apart from minimizing mutual Hamming correlation between patterns, hits resulting from presence of all the sequences in the system should be minimized. This prompts us to define a generalized Hamming correlation function which depends on all the sequences in the family, unlike Hamming correlation which depends on only on two sequences. It is defined as follows.

Let  $\{S^i, m = 1, \dots, n\}$  be a set of  $n$  sequences of length  $L$  over certain alphabet  $\mathcal{A}$ . Then the generalized Hamming crosscorrelation function concerning  $m^{\text{th}}$  sequence is given by

$$\text{GCH}_m(\tau_1, \tau_2, \dots, \tau_{m-1}, \tau_{m+1}, \dots, \tau_n) = \sum_{i=0}^{L-1} \text{gh}\{S^m_i; S^j_{i+\tau_j}, \text{ for all } j \neq m\} \quad (7.1.1)$$

The corresponding autocorrelation function is given by.

$$\text{GAH}_m(\tau_1, \tau_2, \dots, \tau_n) = \sum_{i=0}^{L-1} \text{gh}\{S^m_i; S^j_{i+\tau_j}, \text{ for all } j\} \quad (7.1.2)$$

where  $\text{gh}$  is a function given by

$$\begin{aligned} \text{gh}\{a; b_1, b_2, \dots, b_n\} &= 1 \text{ if } a \in \{b_1, b_2, \dots, b_n\} \\ &= 0 \text{ other wise.} \end{aligned}$$

For proper asynchronous multi-user operation of SFH M-A systems, it required that each code sequence should satisfy following requirements:

1. Generalized Hamming autocorrelation function should have two levels; a large value for inphase correlation and a small value for out-of-phase correlation.
2. Generalized Hamming crosscorrelation function should have a small value.

**Remark 7.1.1:** In fast frequency hopping M-A systems, baseband symbol rate is much smaller than the hopping rate. This means that same symbol will be transmitted in  $k$  frequency hops (Diversity is  $k$ ),  $k > 1$ . Thus even if hit takes place at any hop, information due to the symbol is not lost completely. Thus during design of fast frequency hopping patterns, it is customary to consider only mutual Hamming correlation properties. However, the number of users for multiple access is limited by the frequency diversity.

## 7.2 Construction of Frequency Hopping patterns from Sequences over Orthogonal Ideals of $P_p^n[w(\xi)]$

In this section, properties of orthogonal ideals of polynomial residue class ring are used to construct sequences with ideal generalized Hamming correlation properties (crosscorrelation function is equal to zero for all values of  $\tau_i$ , refer (7.1.1)). Construction of hopping patterns is based on the internal direct sum representation of the ring  $P_p^n[w]$ . The decomposition of the ring  $P_p^n[w(\xi)]$  is given in Appendix F.

In the following we consider  $P_p^n[w(\xi)]$  with  $w(a) = w_1(\xi)w_2(\xi)$ , where  $w_1(\xi)$  and  $w_2(\xi)$  are pairwise relatively prime polynomials. Let  $\deg(w_1(\xi)) = n_1$ ;  $\deg(w_2(\xi)) = n_2$ . Then  $P_p^n[w(\xi)]$  can be written as a direct sum of rings  $P_p^{n_1}[w_1(\xi)]$  and  $P_p^{n_2}[w_2(\xi)]$ . Let  $e_1(\xi)$  and  $e_2(\xi)$  be orthogonal idempotent polynomial corresponding to rings  $P_p^{n_1}[w_1(\xi)]$  and  $P_p^{n_2}[w_2(\xi)]$  respectively. Then ideals  $\langle e_1(\xi) \rangle$  and  $\langle e_2(\xi) \rangle$  are isomorphic to rings  $P_p^{n_1}[w_1(\xi)]$  and  $P_p^{n_2}[w_2(\xi)]$  respectively. From the representation of  $P_p^n[w(\xi)]$  it is clear that the elements of  $\langle e_1(\xi) \rangle$  and  $\langle e_2(\xi) \rangle$  are distinct. Lemma 7.2.1 constructs cosets of  $\langle e_1(\xi) \rangle$  in  $P_p^n[w(\xi)]$ .

**Lemma: 7.2.1:** Cosets of  $\langle e_1(\xi) \rangle \equiv P_p^{n_1}[w_1(\xi)]$  in the ring  $P_p^n[w(\xi)]$  are formed by adding unique elements of  $\langle e_2(\xi) \rangle$  to the ideal  $\langle e_1(a) \rangle$ . Cosets are given by

$$\{a + \langle e_1(\xi) \rangle\} = \{a + x : x \in \langle e_1(\xi) \rangle \equiv P_p^{n_1}[w_1(\xi)]\}$$

for all  $a \in \langle e_2(\xi) \rangle \equiv P_p^{n_2}[w_2(\xi)]$ .

**Proof:** It is easily verified that the cosets are distinct. Also, each coset of  $\langle e_1(\xi) \rangle$  contains a unique element from  $\langle e_2(a) \rangle$ . If not so, then we have,  $x_1 \neq 0$  and  $x_1 \in \langle e_1(\xi) \rangle$  such that

$$a + x_1 = b, \text{ with } a \neq b, a, b \in \langle e_2(a) \rangle$$

This implies that  $a - b = x_1$  is a non-zero element of  $\langle e_1(a) \rangle$  thus leading to a contradiction.  $\square$

Sequences with ideal generalized Hamming correlation properties are constructed using cosets of  $\langle e_1(\xi) \rangle$  defined above. Elements corresponding to each sequence are drawn from a distinct coset. Since these cosets are mutually exclusive (there are no common elements among these cosets), ideal generalized Hamming correlation properties follow naturally. Optimal families sequences over  $P_p^n[w^k]$  given in Chapter 4 are used to construct sequences with ideal generalized Hamming correlation properties.

## 7.2.1 Construction of Sequences with Ideal Generalized Hamming Correlation Properties

In this section, a construction of sequences over  $P_p^n[w(\xi)]$  of length  $p^{n_1} - 1$  is described by making use of a sequence over  $P_p^{n_1}[w_1(\xi)]$ . As given in Lemma 7.1,  $P_p^n[w(\xi)]$  consists of  $p^{n_2}$  cosets of  $\langle e_1(a) \rangle = P_p^{n_1}[w_1(\xi)]$ . We make use of these cosets in the construction of sequences with ideal generalized Hamming correlation properties. Each sequence over  $\langle e_1(a) \rangle$  is assigned to a unique coset of  $\langle e_1(a) \rangle$  in  $P_p^n[w(\xi)]$ .

**Theorem 7.2.1: (Code Construction Theorem)** Let  $S^A = \{s_i\}$  be a sequence over  $P_p^{n_1}[w_1(\xi)]$  of period  $p^{n_1} - 1$  which has optimal Hamming autocorrelation properties. A set of  $V = p^{n_2}$  sequences of length  $L = p^{n_1} - 1$  over  $P_p^n[w(\xi)]$  can be generated as follows. Associated with an element of  $A_j(\xi)$  of  $P_p^{n_2}[w_2(\xi)]$ ,  $0 \leq j < p^{n_2}$ , a sequence over  $P_p^n[w(\xi)]$ ,  $F^j$  is defined as

$$\begin{aligned} F^j &= \{F_i^j, i = 0, 1, \dots, p^{n_1} - 1\} \\ F_i^j &= s_i(\xi)e_1(\xi) + A_j(\xi)e_2(\xi) \end{aligned} \quad (7.2.1)$$

where  $e_1(\xi)$  and  $e_2(\xi)$  are idempotent generators of ideals in  $P_p^n[w(\xi)]$ . The generalized Hamming crosscorrelation function of  $F^j$  is given by

$$GCH_{F^j}(\tau_1, \tau_{j-1}, \tau_{j+1}, \dots, \tau_u) = 0 \text{ for all } \tau_i \neq \tau_j \quad (7.2.2)$$

and its corresponding autocorrelation function is given by

$$GAH_{F^j}(\tau_1, \tau_2, \dots, \tau_n) = AH_A(\tau_j) \quad (7.2.3)$$

**Proof:** From internal direct sum representation of  $P_p^n[w(\xi)]$ ,  $F_i^j$  belongs to a coset of  $\langle e_1(\xi) \rangle$  associated with the element  $A_j(\xi)e_2(\xi) \in \langle e_2(\xi) \rangle$ . Since the cosets are mutually exclusive ideal crosscorrelation properties follow. Using this equation in (7.1.2) gives (7.2.3).  $\square$

**Example 7.2.1:** Sequences are defined over  $P_2^6[w(\xi)]$ ; where  $w(a) = w_1(\xi)w_2(\xi)$ ;  $w_1(\xi) = (1 + \xi + \xi^3)$ ,  $w_2(\xi) = (1 + \xi^2 + \xi^3)$ .

Number of sequences in the set  $= 2^3 = 8$ .

Length of sequences in the set  $= 7$ .

Each sequence element is represented by an integer  $< 63$  which is the decimal representation of an element of  $P_2^6[w(\xi)]$ . (evaluation of polynomial  $\in P_2^6[w(\xi)]$  at  $\xi=2$ ). Sequences are given in Table 7.2.1.



Table 7.2.1 Sequences for Example 7.2.1

---

Sequence $S^0$	{ 52, 46, 23, 35, 13, 26, 57}
Sequence $S^1$	{ 22, 12, 53, 01, 47, 56, 27}
Sequence $S^2$	{ 54, 44, 21, 33, 15, 24, 59}
Sequence $S^3$	{ 25, 03, 58, 14, 32, 55, 20}
Sequence $S^4$	{ 48, 42, 19, 39, 09, 30, 61 }
Sequence $S^5$	{ 08, 18, 43, 31, 49, 38, 05}
Sequence $S^6$	{ 37, 63, 06, 50, 28, 11, 40}
Sequence $S^7$	{ 16, 10, 51, 07, 41, 62, 29}

---

The generalized Hamming correlation properties of sequences in the above theorem depend on the Hamming autocorrelation properties of sequence  $S^A$  used in the construction. Also, a single sequence ( $S^A$ ) over  $P_p^n[w_1(\xi)]$  is used in the above construction. Since the crosscorrelation properties mainly follow from the coset structure of  $P_p^n[w(\xi)]$ , it is possible to consider different sequences while constructing sequences over different cosets of  $P_p^n[w(\xi)]$ . Such a SFH M-A communication system is considered below. The coset structure ensures certain slots for a particular user. In the M-A communication considered, frequency slots in which any user transmits his message is represented by an element in  $P_p^n[w(\xi)]$  and each user is assigned with slots indicated by a distinct coset. The general arrangement for sequence generation is given Fig. 7.2.1.

In the above M-A system total of frequency slots available are  $p^n$ , the order of  $P_p^n[w(\xi)]$ . Each user can use  $p^{n-1}$  slots. Thus frequency expansion factor for any  $i^{\text{th}}$  user is  $K_i = p^{n-1}$ . Even if any particular user occupies some fraction of the total available frequency slots, individual frequency slots are distributed in the entire band of spectrum available. Hence virtually each user occupies entire frequency spectrum of M-A system.

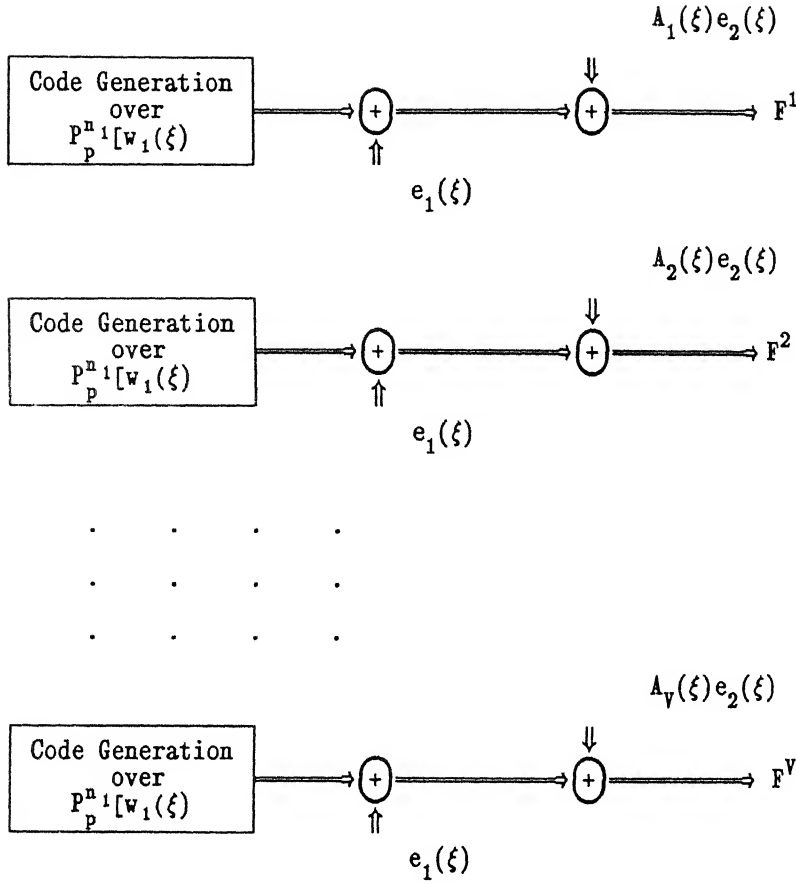


Fig 7.2.1: A Code Generation Arrangement for Slow Hopping M-A Communication Environment

### 7.3 Construction of Set of Hopping Patterns over $P_p^n[w(\xi)]$ from One-coincidence Sequences over $P_p^{n-1}[w_1]$

In the code construction of Section 7.2, the elements of any sequence  $F^{(j)}$  belong to a distinct coset. Hence number of sequences are limited by the number cosets in the ring  $P_p^n[w(\xi)]$ . If a larger set of sequences is required, then the requirements on the ideal generalized hamming correlation properties of sequences need to be relaxed. In the following we give one such construction using one-coincidence sequences  $P_p^{n-1}[w_1]$  of length  $p^{n-1}-1$ . Before doing that, let us calculate the generalized Hamming correlation properties of one-coincidence sequences.

**Lemma 7.3.1:** A set of  $\mu$  one-coincidence sequences over  $P_p^{n_1}[w_1]$  of length  $p^{n_1} - 1$  has following generalized correlation values.

$$\begin{aligned} \text{GAH}_{Fj}(\tau_j, \tau_1, \dots, \tau_{j-1}, \tau_{j+1}, \dots, \tau_u) &\leq p^{n_1} - u, \text{ for } \tau_j = 0 \\ &\leq u-1, \text{ otherwise} \end{aligned} \quad (7.3.1)$$

$$\text{GCH}_{Fj}(\tau_1, \tau_{j-1}, \tau_{j+1}, \dots, \tau_u) \leq u-1 \text{ for all } \tau_i \neq \tau_j \quad (7.3.2)$$

**Proof:** Generalized Hamming crosscorrelation concerning  $m^{\text{th}}$  sequence can be written as

$$\begin{aligned} \text{GCH}_m(\tau_1, \tau_2, \dots, \tau_{m-1}, \tau_{m+1}, \dots, \tau_n) &= \sum_{i=0}^{L-1} \text{gh}\{S_i^m; S_{i+\tau_j}^j, \text{ for all } j \neq m\} \\ &= \sum_{i=0}^{L-1} h(S_i^m; S_{i+\tau_1}^1) \text{ OR } \dots \text{ OR } h(S_i^m; S_{i+\tau_{m-1}}^{m-1}) \text{ OR } h(S_i^m; S_{i+\tau_{m+1}}^{m+1}) \dots \text{ OR } h(S_i^m; S_{i+\tau_u}^u) \end{aligned}$$

where  $h$  is the Hamming function given by

$$\begin{aligned} h\{a; b\} &= 1 \text{ if } a = b \\ &= 0 \text{ other wise.} \end{aligned}$$

Hamming crosscorrelation between any two one-coincidence sequences is at most one.  $\text{GCH}_{A^j}(\tau)$  is the total number of coincidences for  $A^j$  with  $u-1$  other sequences. Hence at the maximum correlation value can be  $u-1$  which proves (7.3.2). Similarly (7.3.2) (autocorrelation bound) also can be proved.  $\square$

In the following construction,  $\mu$  one-coincidence sequences are employed in each coset increasing the total number of sequences to  $\mu p^{n_2}$ .

**Theorem 7.3.1:** A set of  $V = \mu p^{n_2}$  sequences of length  $L = p^{n_1} - 1$  over  $P_p^{n_1}[w(\xi)]$  can be generated as follows. Let  $\{S(l), l = 1, \dots, \mu\}$  be a set of  $\mu$  one-coincidence sequences over  $P_p^{n_1}[w_1(\xi)]$ , then a set of  $\mu p^{n_2}$  are given by the set

$$\begin{aligned} \{F^{(j,m)}, j = 0, 1, \dots, \mu, m = 1, \dots, p^{n_2}\}; F^{(j,m)} &= \{F^{(j,m)}_i, i \in Z_L \\ F^{(j,m)}_i &= s_i(\xi)e_1(\xi) + A_m(\xi)e_2(\xi) \end{aligned}$$

where  $\{s_i: i=0, 1, \dots, p^{n_1} - 1\} = S(j)$ ,  $j^{\text{th}}$  one-coincidence sequence and  $A_m(\xi)$  is unique in  $P_p^{n_2}[w_2(\xi)]$ ,  $m=0, \dots, p^{n_2}-1$ .

Generalized Hamming properties are given by

$$\begin{aligned} \text{GAH}_{F(m,j)}(\tau_j, \tau_1, \dots, \tau_{j-1}, \tau_{j+1}, \dots, \tau_u) &< p^{n_1} - \mu \text{ for } \tau_j = 0 \\ &< \mu - 1, \text{ otherwise} \end{aligned} \quad (7.3.3)$$

$$\text{GCH}_F(j)(\tau_1, \tau_{j-1}, \tau_{j+1}, \dots, \tau_u) < \mu - 1, \text{ for all } \tau_i \neq \tau_j \quad (7.3.4)$$

Proof: Proof runs similar to the construction in Theorem 7.2.1 except that here elements from  $\mu$  sequences belong to a distinct coset. Autocorrelations and crosscorrelations follow from the properties of the one-coincidence sequences (Lemma 7.3.1) used in the construction.  $\square$

## 7.4 Construction of Sequences with Variable Frequency Expansion Factors

Frequency expansion factor (diversity) for different users in the above constructions are uniformly  $p^{n_1}$ . A situation is considered where different users can have different frequency expansion factors in this section. Let us consider again the ring  $P_p^n[w(\xi)]$ ,  $w(a) = w_1(\xi)w_2(\xi)$ . According to Lemma 7.2.1,  $P_p^n[w(\xi)]$  consists of  $p^{n_2}$  cosets of  $\langle e_1(\xi) \rangle \equiv P_p^{n_1}[w_1(\xi)]$ . When  $w_1(\xi)$  has factors which are pair wise relatively prime, then we can divide a coset of  $\langle e_1(\xi) \rangle$  into cosets of its subrings. These cosets contain less elements than the cosets of  $\langle e_1(\xi) \rangle$ . Sequences are then defined over these smaller cosets. Thus frequency slots available to different users can be varied. This way different users can have different frequency expansion factors.

In the following we describe M-A system where different users will have different  $K_i$ . Let  $w(a) = w_1(\xi)w_2(\xi)$  where  $w_1(\xi)$  and  $w_2(\xi)$  are pair wise relatively prime with  $\deg(w_1(\xi)) = n_1$ ,  $\deg(w_2(\xi)) = n_2$ . Let

$$w_1(a) = y_1(\xi)y_2(\xi)\dots y_r(\xi).$$

$\deg(y_i(\xi)) = m_i$ . Let  $ye_1(\xi)$ ,  $ye_2(\xi)$ , ...,  $ye_r(\xi)$  be idempotent polynomials in  $P_p^n[w(\xi)]$  corresponding to sub rings  $P_p^{m_i}[y_i(\xi)]$ ,  $1 \leq i \leq r$ . Then from Appendix F

$$e_1(a) = ye_1(\xi) + ye_2(\xi) + \dots + ye_r(\xi) \text{ and}$$

$$P_p^n[w(\xi)] = \langle ye_1(\xi) \rangle \oplus \langle ye_2(\xi) \rangle \oplus \dots \oplus \langle ye_r(\xi) \rangle \oplus \langle e_2(\xi) \rangle,$$

where  $\oplus$  represents internal direct sum symbol.

$$\text{Let } u_i(\xi) = \prod_{j=1}^i y_j(\xi), 1 \leq i \leq r \text{ and}$$

$$\bar{u}_i(\xi) = \prod_{j=i}^r y_j(\xi), 0 \leq i \leq r.$$

Let  $d_i$  and  $\bar{d}_i$ ,  $1 \leq i \leq r$ , be the degrees of  $u_i(\xi)$  and  $\bar{u}_i(\xi)$  respectively. Let the idempotent polynomials corresponding to rings  $P_p^{d_i}[u_i(\xi)]$  and  $P_p^{\bar{d}_i}[\bar{u}_i(\xi)]$ ,  $1 \leq i \leq r$ , in  $P_p^n[w(\xi)]$  be  $ue_i(\xi)$  and  $\bar{ue}_i(\xi)$  respectively. Then from the internal direct sum structure (Appendix F), following follows.

$$\begin{aligned}
ue_i(\xi) &= \sum_{j=1}^i ye_i(\xi) \\
d_i &= \sum_{j=1}^i m_j \\
\overline{ue}_i(\xi) &= \sum_{j=i}^r ye_i(\xi) \\
\overline{d}_i &= \sum_{j=i}^r m_j \\
eu_i(\xi) + \overline{ue}_i(\xi) &= e_i(\xi)
\end{aligned}$$

With the above configuration,  $r$  different user groups can be identified. Users of  $i^{\text{th}}$  user group are assigned frequency slots corresponding to cosets of  $\langle ue_i(\xi) \rangle \equiv P_p^{d_i}[u_i(\xi)]$ . There are  $p^{n_1-d_i}$  cosets of  $\langle ue_i(\xi) \rangle$  in each coset  $\langle e_i(\xi) \rangle$ . The  $i^{\text{th}}$  group of users are assigned with unique cosets of  $\langle e_i(\xi) \rangle$ . Thus number of possible users for  $i^{\text{th}}$  group is integer multiple of  $p^{n_1-d_i}$ . Code construction arrangement is shown in the Fig 7.4.1. Frequency expansion factor for each user in the  $i^{\text{th}}$  group is  $k_i = p^{d_i}$ .  $B_j^i(\xi)\overline{ue}_i(\xi) + A_i(\xi)e_2(\xi)$  constitutes address for  $j^{\text{th}}$  sequence in  $i^{\text{th}}$  user group.

M-A system given above is a generalized arrangement to the one given in Sec. 7.2. In the present case, alphabet size for different users are different. Hence the sequence length of different users can be different. Sequences constructed in Chapter 4 can be used in this M-A arrangement. Since sequences thus defined belong to a unique coset in  $P_p^n[w(\xi)]$ , ideal generalized Hamming correlation properties follow as in Sec. 7.2.

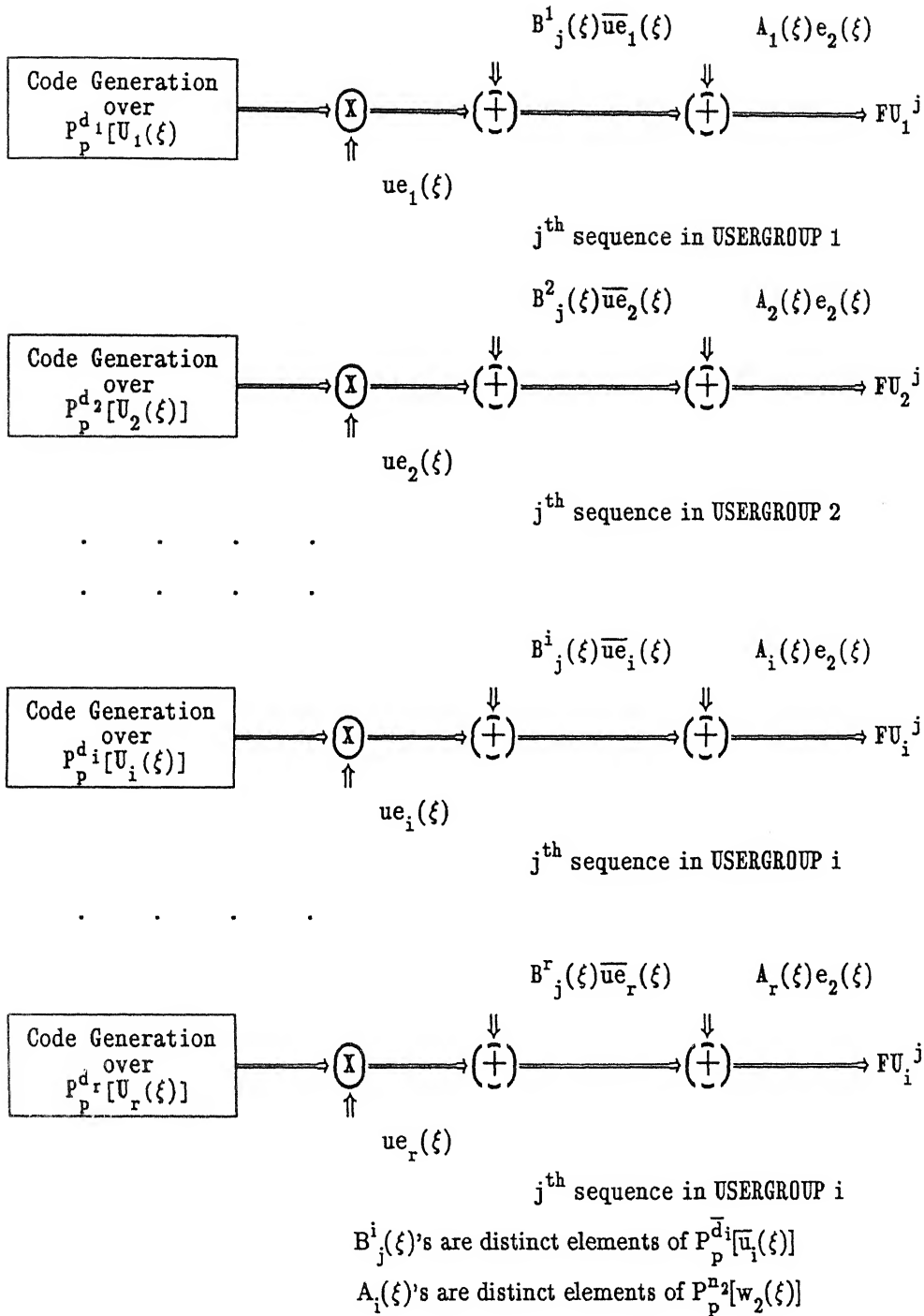


Fig. 7.4.1 Code Generation Arrangement for Slow Hopping M-A system with Users Having different Frequency Expansion Factors

*Example 7.4.1:*  $w(\xi) = w_1(\xi)w_2(\xi) = 0 + \xi + \xi^2 + \xi^5 + \xi^7$ .

$y_1(\xi) = (1 + \xi + \xi^3)$ ,  $y_2(\xi) = (1 + \xi)$ ,  $y_3(\xi) = (0 + \xi)$ ,  $w_2(\xi) = (1 + \xi + \xi^2)$ .

$u_1(\xi) = (1 + \xi + \xi^3)$ ;  $u_2(\xi) = (1 + \xi + \xi^3)(1 + \xi)$ ;  $u_3(\xi) = (1 + \xi + \xi^3)(\xi + \xi^2)$ ;

Total Number of frequency slots available = 128.

Elements of  $P_p^n[w(\xi)]$  are represented in this example by decimal numbers between 0–127;  $a(\xi) \in P_p^n[w(\xi)]$  is represented by the number  $a(\xi)$  evaluated at  $\xi = 2$ .

Number of User Groups = Number of factors of  $w_1(\xi) = 3$ .

Idempotent polynomial  $ye_1(a) = 0 + \xi + \xi^2 + \xi^3 + \xi^4 + \xi^5 + \xi^6$ .

Idempotent polynomial  $ye_2(\xi) = 0 + \xi + \xi^5 + \xi^6$ .

Idempotent polynomial  $ye_3(\xi) = 1 + \xi + \xi^4 + \xi^6$ .

Idempotent polynomial  $e_2(\xi) = 0 + \xi + \xi^2 + \xi^3 + \xi^6$ .

User Group No 1:

Number of users in this group : 4;

Frequency expansion factor : 8;

Sequence idempotent polynomial :  $eu_1(\xi) = 0 + \xi + \xi^2 + \xi^3 + \xi^4 + \xi^5 + \xi^6$ .

Alphabet for the sequence construction :  $\langle eu_1(\xi) \rangle \equiv P_2^3[u_1(\xi)]$

Frequency Slots for  $U_1^1$  — 116, 10, 46, 80, 102, 24, 60, 66.

corresponding address is —  $0 + \xi^2 + \xi^4 + \xi^5 + \xi^6$

Frequency Slots for  $U_2^1$  — 39, 89, 125, 3, 53, 75, 111, 17.

corresponding address is —  $1 + \xi + \xi^2 + \xi^5$

Frequency Slots for  $U_3^1$  — 22, 104, 76, 50, 4, 122, 94, 32.

corresponding address is —  $0 + \xi + \xi^2 + \xi^4$

Frequency Slots for  $U_4^1$  — 69, 59, 31, 97, 87, 41, 13, 115.

corresponding address is  $1 + \xi^2 + \xi^6$

User Group No 2:

Number of users in this group : 2;

Frequency expansion factor : 16;

Alphabet for the sequence construction:  $\langle eu_2(\xi) \rangle \equiv P_2^4[u_2(\xi)]$

Sequence idempotent polynomial  $ue_2(\xi) = 0 + \xi^2 + \xi^3 + \xi^4$ .

Frequency Slots for  $U_1^2$  — 58, 38, 2, 30, 74, 86, 114, 110, 124, 96, 68, 88, 12, 16, 52, 40.  
 corresponding address is —  $0 + \xi + \xi^3 + \xi^4 + \xi^5$ .

Frequency Slots for  $U_2^2$  — 105, 117, 81, 77, 25, 5, 33, 61, 47, 51, 23, 11, 95, 67, 103, 123.  
 corresponding address is —  $1 + \xi^3 + \xi^5 + \xi^6$ .

User Group No 3:

Number of users in this group : 2;

Frequency expansion factor : 32;

Alphabet for the sequence construction:  $\langle eu_3(\xi) \rangle \equiv P_2^5[u_3(\xi)]$

Sequence idempotent polynomial :  $ue_3(\xi) = 1 + \xi + \xi^2 + \xi^3 + \xi^6$ .

Frequency Slots for  $U_1^3$ .

0, 79, 56, 119, 112, 63, 72, 7, 70, 9, 126, 49, 54, 121, 14, 65, 42, 101, 18, 93, 90, 21, 98, 45, 108, 35, 84, 27,  
 28, 83, 36, 107.

corresponding address is  $0 +$

Frequency Slots for  $U_2^3$ :

78, 1, 118, 57, 62, 113, 6, 73, 8, 71, 48, 127, 120, 55, 64, 15, 100, 43, 92, 19, 20, 91, 44, 99, 34, 109, 26, 85,  
 82, 29, 106, 37.

corresponding address is  $0 + \xi + \xi^2 + \xi^3 + \xi^6$ .



## Chapter 8

### Conclusions

In this chapter we briefly summarize the results obtained in the thesis and suggest some research topics which can be studied on the lines of the approach taken here.

#### 8.1 Summary of Results

We have studied algebraic constructions of sequences obtained from residue class finite rings and periodic correlation and linear complexity (LC) properties of such sequences. Such sequences are of interest in polyphase and frequency hopping code division multiple-access (CDMA) communication systems. The finite rings considered in the study are:

- Residue class integer ring modulo  $2^k$ :  $Z_{2^k}$ , where  $k$  is a positive integer.
- Residue class polynomial ring  $GF(p)[\xi] \bmod w(\xi)$ :  $P_p^n[w(\xi)]$ , where  $w(\xi)$  is an  $n^{\text{th}}$  degree polynomial over  $GF(p)$ .

Mainly local rings have been considered in the study since any general semi-local ring can be expressed as a direct sum of local rings. The study includes generalizations of (i) sequence construction mechanisms and (ii) evaluation of correlation and LC parameters of constructed sequences. Sequence generation mechanisms using polynomial functions of trace sequences over finite fields have been generalized to residue class finite rings. Trace functions over Galois extension rings have been defined using automorphisms of Galois extension rings. The sequences are defined as generalized polynomial functions of trace functions over Galois extension rings. This generalization has resulted in a large number of families of sequences. Galois extension of residue class rings plays a similar role here as Galois fields for finite field case. Several novel methods for computation of periodic correlation properties (correlation values and their distribution) of constructed sequences are given. These are

- 1) use of an Abelian association scheme on the elements of the Galois extension ring of  $Z_4$  for computation of periodic correlation properties of sequences over  $Z_4$ .
- 2) use of generalized trace functions and vector space properties of Galois extensions of polynomial residue class rings for computation of correlation properties of sequences over polynomial residue class rings.

A generalization of Blahut's complexity theorem for computing LC of sequences over finite fields, as applicable to sequences over residue class rings, has been used to compute the LC of constructed sequences.

The approach used to obtain sequences over residue class rings is named as structural approach since the sequences are constructed over a finite alphabet purely from the structural properties of the finite alphabet. These sequences are transformed into real (or complex) signals through an appropriate mapping  $\phi$  from finite alphabet to a subset of real (or complex) numbers called signal set. Suitability of these sequences depends on the properties of transformed sequences and hence a major effort is devoted to this aspect. Properties of sequences are classified into primary and secondary properties. Properties, like linear complexity, period and  $r$ -tuple distributions, depend on structure of the finite alphabet and are termed as primary, while properties like correlation functions depend on the mapping used from finite alphabet to appropriate signal set and are termed as secondary. In the structural approach, secondary properties are difficult to control although they are critical in practice whereas primary properties are better controlled due to their immediate relation with their sequence generation mechanisms. A generalized correlation function between a pair of sequences over a finite alphabet is defined to take care of various correlation functions of practical importance such that the specific correlation functions can be derived from it as special cases. The generalized correlation function is characterized by  $\phi$ , a mapping from a finite alphabet to an appropriate signal set, and  $f$ , a binary operation which depends on correlation type and distance measure. Various correlation functions considered are binary, quaternary, and  $m$ -ary inner-product correlations, Hamming and Lee correlations, and block inner-product correlations. Using the generalized correlation function, a notion of finite ring alphabet matched to a signal set for a correlation is put forward in an attempt to ease the secondary analysis. In this notion, correlation operation  $f$  is isomorphic to subtraction in the finite ring alphabet and more importantly the mapping is linear. This allows us to make use of linearity in the ring domain for the evaluation of correlation properties of constructed sequences. The matching concept accordingly permits us to retain the advantages of linearity which in turn simplifies the analysis of sequences. Several finite rings are identified which are matched to various correlation functions and they are utilized to construct many optimal families of sequences.

Equivalences of some correlation functions are also discussed in the thesis. A definition of equivalence is given and it is shown that Hamming correlations are equivalent to binary inner-product correlations and block binary Hamming correlations are equivalent to block binary inner-product correlations.

We have also considered generalized Hamming correlation functions which depend on all the sequences employed in the system. They are useful in slow frequency hopping communication systems.

Main results given in the thesis are summarized below:

Various families of sequences derived in the thesis are classified into two categories: a) Families derived from local rings, b) Families derived from semi-local rings. Sequence constructions make use of following two important Galois extension rings

- Galois extension ring of  $Z_{2^k}$  of degree of extension  $r$ , denoted by  $GR(2^k, r)$ .
- Galois extension ring of  $P_p^n[w^k]$ , denoted by  $PGR(V^k, r)$ , where  $V$  represents the residue field  $P_p^m[w]$  of order  $p^m$  isomorphic to  $GF(p^m)$ .

Major constructions of sequences given in the thesis are:

I) Trace sequences: Using trace functions from Galois extension rings to one of its intermediate subrings, families of sequences called trace sequence families are defined using unit elements of Galois extension rings. These sequences are linear in the sense that sequences in a family are closed under pointwise ring addition. A family of trace sequences over a local ring also includes families of trace sequences over the ring ideals since a local residue class ring contains a chain of local ideals. The period of a trace sequence is determined by the multiplicative order of the unit element  $\alpha$  used to define the family. The group of units of a Galois extension ring is in general Abelian which has a cyclic component group  $G_c$  isomorphic to the group of units of its residue field. An unit element  $\alpha$  of the cyclic component group is called a primitive element if its multiplicative order is same as the order of the cyclic component group. The family of trace sequences is called a family of  $m$ -sequences or simply  $\mathcal{N}$  family if the unit element  $\alpha$  used to define the family is a primitive unit element of the Galois extension ring. The main difference between finite field and finite ring  $m$ -sequences is that there is only one cyclically distinct field  $m$ -sequence for a primitive element  $\alpha$  of  $GF(2^r)$ , whereas in the ring case there is a family of  $m$ -sequences corresponding to an element  $\alpha$  of the extension ring. Families of sequences constructed using trace functions are:

- 1) families of quadriphase sequences derived from  $m$ -sequences and interleaved  $m$ -sequences over  $Z_4$ ,
- 2) families of octaphase sequences derived from  $m$ -sequences over  $Z_8$ ,
- 3) families of frequency hopping patterns derived from  $m$ -sequences over  $P_p^n[w^k]$ .

II) Generalized polynomial sequences with controllable linear complexity: A method of obtaining controllable linear complexity using polynomial sequences over finite fields [47] has been generalized to residue class rings. A complexity enhancement procedure is given. The scheme makes use of generalized permutation polynomials over appropriate Galois extension rings. Generalizations of permutation monomials over Galois extension rings are considered and accordingly families of GGMW sequences over  $Z_4$  and  $P_p^n[w^k]$  are defined. Families derived using this method are:

- 1) Families of quadriphase sequences derived from GGMW sequences of period  $2^{ru}-1$ ,  $r$  and  $u$  being positive integers,
- 2) Families of frequency hopping patterns derived from a subset of GGMW sequences over  $P_p^n[w^k]$ .

III) Sequences obtained from mappings from a ring to its ideal: Nonlinear polynomial mappings from  $Z_4$  to its proper ideal  $\langle 2 \rangle$  have been employed to define families of biphasic sequences. Families obtained under this method are families of biphasic sequences derived from  $m$ -sequences and interleaved  $m$ -sequences over  $Z_4$ .

IV) Sequences over semi-local ring  $P_p^n[w(\xi)]$ : Internal direct sum representation of  $P_p^n[w(\xi)]$  has been employed to define sequences over semi-local rings  $P_p^n[w(\xi)]$ , where  $w(\xi)$  is a composite polynomial of degree  $n$ . The ring  $P_p^n[w(\xi)]$  is divided into different cosets of its subring and sequences are defined over these cosets. The resultant sequences have ideal generalized Hamming correlation properties. These families are useful in slow frequency hopping multiple-access communication systems.

Important methods employed to determine the properties of constructed sequences are as follows.

- 1) An Abelian association scheme on the elements of  $GR(4, r)$  has been employed to determine crosscorrelation properties of maximal length sequences and interleaved maximal length sequences over  $Z_4$ .
- 2) Vector space properties of  $PGR(V^k, r)$  and trace functions over  $PGR(V^k, r)$  are employed to determine the Hamming correlation properties of sequences over  $P_p^n[w^k]$ .
- 3) Linear complexity computations for sequences over rings derived in the thesis use generalized version of Blahut's complexity theorem for sequences over finite field. The theorem makes use of generalized Fourier transform representation of sequences over rings.

## 8.2 Suggestions for Further Work

In the study of sequences Galois extension rings provide a general setting in which sequences over  $GF(p)$ ,  $GF(p^r)$ ,  $Z_{p^k}$  and  $P_p^n[w^k]$  appear as special cases. While lot of results exist for Galois fields in the context of study of sequences, very few results are available for  $Z_{p^k}$  and  $P_p^n[w^k]$ . In this study we have considered rings  $Z_4$ ,  $Z_8$  and  $P_p^n[w^k]$  and many new constructions of families of sequences are given. With the rich structure of Galois rings, many more new constructions might be possible. Many algebraic properties of sequence construction methods will carry over to other rings also. It would be interesting to pursue work in this general direction. Specifically, we suggest following topics for further research.

- 1) In this thesis we considered only periodic correlation properties of sequences. In practical systems several other parameters of sequences like aperiodic correlations, run length distributions, even and odd correlations are important. Analytical evaluation of these parameters may be difficult and for most of the previously known sequences a recourse to computer simulation is taken. A similar approach using computers may be taken up for evaluation of these practically relevant parameters for optimal families of sequences derived in this thesis.
- 2) Abelian association scheme considered in this thesis applies only to  $GR(4,r)$  and they were used in the evaluation of correlation parameters of  $m$ -sequences over  $Z_4$ . The idea can be extended easily to  $GR(2^k,r)$  and  $GR(p^k,r)$  where  $p$  is a prime and  $k$  is any positive integer. These results then could be used to compute correlations of  $m$ -sequences over  $Z_{2^k}$  and  $Z_{p^k}$ , but the complexity of combinatorial computations is expected to increase exponentially with  $k$ . It is indeed a challenging problem for further research.
- 3) Generalizations of polynomial functions of trace sequences over finite fields to residue class rings constitute the important sequence construction methods used in this thesis. Other sequence construction methods over finite fields like construction of bent function sequences could also be generalized.
- 4) Frequency hopping patterns are constructed from residue class polynomial rings in this thesis. Patterns could also be constructed from sequences over residue class integer rings. Some of the necessary results, like weight distribution of  $m$ -sequences over  $Z_4$ , towards this are already present in the thesis. These can be used to compute Hamming correlation properties of constructed patterns. Computation of Hamming correlation properties of general  $m$ -sequences over  $Z_{p^k}$  is an interesting problem.

- 5) It is shown in the thesis that binary Hamming correlation function is equivalent to biphasic inner-product correlation function. This fact is responsible for efficient realization of biphasic synchronization schemes through binary Hamming correlation functions [36]. Lee correlation is a counterpart of Hamming correlation for MPSK modulation. However, Lee correlation is not equivalent to MPSK inner-product correlations. Wolf [80] has shown that MPSK channel is matched to Lee metric and hence there is a possibility that distinguishability measures of Lee and MPSK inner-product correlations are related. It is worthwhile to investigate importance of Lee correlation in implementation of synchronization schemes for MPSK spread spectrum communication systems.
- 6) We have stated a conjecture (Section 5.2.2) for characterizing correlation preserving permutations in complexity enhancement procedure for sequences over  $Z_4$ . We feel that the theory of association schemes can be used to prove the result. It is an interesting problem for further investigation.
- 7) We have given a multiple-access system using slow frequency hopping patterns derived in the thesis. Detailed study of topics like noise immunity and practical viability of such systems is needed.
- 8) Some of the algebraic tools developed in the thesis can be used to study codes over rings. For example, negacyclic codes over  $Z_4$  of length  $2^r-1$  can be studied using Galois extension ring  $GR(4,r)$ . Generator polynomial of a negacyclic code of length  $2^r-1$  is a factor of the polynomial  $x^{2^r-1}+1$ , and elements of order  $2(2^r-1)$  in  $GR(4,r)$  are the roots of this polynomial. Investigations in this direction may give fruitful results.
- 9) Block inner-product correlations are studied in connection with only residue class polynomial rings in this thesis. Same idea could be extended to polynomial residue class rings of  $Z_M$ .
- 10) The thesis does not discuss cryptographic implications of the results directly. However, some of the constructed sequences can be used in cryptographic applications also. Requirements for sequences over residue class rings for cryptographic applications need further investigation.
- 11) In this thesis non-linear polynomial mappings from a ring to its ideals have been specifically used to get sequences mainly for use in CDMA. Dai, Beth, and Gollman [85] have considered mappings from residue class rings to  $GF(2)$  for constructing sequences with large LC for cryptographic applications. This topic can be further studied which might lead to interesting applications.

12) Cryptographic systems using the ring  $Z_{mn}$ , where  $m$  and  $n$  are pair wise relatively prime numbers, are common. Similar systems could be constructed based on polynomial residue class ring  $P_p^n[w_1(\xi)w_2(\xi)]$ , where  $w_1(\xi)$  and  $w_2(\xi)$  are pair wise relatively prime polynomials. Polynomial residue class rings are perfectly suited for multiplexing on XOR channels [25]. Thus a multiplexing scheme with cryptographic features can be built using polynomial residue class rings. Studies in this direction might lead to novel cryptographic schemes.

## Appendix A

### Properties of $Z_{2^k}$ and $GR(2^k, r)$

This appendix collects essential mathematical results of the residue class integer ring  $Z_{2^k}$  and its Galois extension ring  $GR(2^k, r)$ , as required for this thesis.

**Definition A.1:** Let  $Z$  be the ring of all integers, and let  $k$  be any positive integer. Then  $Z_{2^k}$  is a residue class integer ring modulo  $2^k$ , denoted by  $Z_{2^k}$ .  $Z_{2^k}$  is a local finite ring.

**Definition A.2:** Galois Ring  $GR(p^k, r)$ : Let  $Z_{2^k}[x]$  be the ring of all polynomials over  $Z_{2^k}$ . Let  $\psi(x)$  be a monic basic irreducible polynomial of degree  $r$  over  $Z_{2^k}$ .  $GR(2^k, r)$  is defined as  $Z_{2^k}[x]/\psi(x)$ ; the residue class polynomial ring  $Z_{2^k}[x] \bmod \psi(x)$  (Set of all polynomials of degree  $r-1$  over  $Z_{2^k}$ ).

#### Construction of $GR(2^k, r)$ :

Choose  $\psi(x)$ , a basic monic irreducible polynomial over  $Z_{2^k}$  such that the multiplicative order of element  $x$  in  $Z_{2^k}[x]/\psi(x)$  divides  $(x^{2^r-1}-1)$  (There always exists such  $\psi(x)$ ). Then  $GR(2^k, r)$  contains elements of the form  $\sum_{i=0}^{r-1} a_i x^i$ ,  $a_i \in Z_{2^k}$ . Alternatively elements of  $GR(p^k, r)$  can be viewed as vectors of length  $r$  over  $Z_{2^k}$ .

#### Structural properties of $GR(2^k, r)$ : [87,88]

**A1.** For every positive integer  $d$ , there is a natural inclusion of  $GR(2^k, r)$  into  $GR(2^k, dr)$ , similar to Galois fields. In other words, every sub ring of the ring  $GR(2^k, r)$  is of the form  $GR(2^k, s)$  for some divisor  $s$  of  $r$ . Conversely, for every positive divisor  $s$  of  $r$ , there is a unique sub ring  $R$  which is isomorphic to  $GR(2^k, s)$ .

**A2.** There is a natural homomorphic mapping from  $GR(2^k, r)$  to  $GR(2^{k-i}, r)$ , for each  $i$ ,  $0 \leq i < k$ , and there are exactly  $r$  such mappings.



Ideal structure of galois rings: [87,88]:

A3. Every ideal in  $GR(2^k, r)$  is generated by an element  $2^i$  and is of the form  $\langle 2^i \rangle = 2^i * GR(2^k, r)$ ,  $0 \leq i \leq k$ . The ideal  $2 * GR(2^k, r)$  is principal. Ideals exhibit the chain property such that elements of  $\langle 2^i \rangle$  is present in all ideals  $\langle 2^j \rangle$ ,  $j < i$ ;

$$\langle 2^k GR(2^k, r) \rangle \subset \langle 2^{k-1} GR(2^k, r) \rangle \subset \dots \subset \langle 2 GR(2^k, r) \rangle \subset \langle GR(2^k, r) \rangle$$

A4. The ideal  $\langle 2^i \rangle$ ,  $0 \leq i \leq k$  is isomorphic to  $GR(2^{k-i}, r)$ .

A5. Every non-zero element of  $GR(2^k, r)$  may be written as  $u2^t$ , where  $u$  is a unit and  $t$  an integer  $0 \leq t \leq k-1$ . In this representation  $t$  is unique and  $u$  is unique modulo  $(2^{k-t})$ .

Group of units of  $GR(p^k, r)$ : [87]

A6. The group of units of  $GR(2^k, r)$ , denoted by  $GR^*(2^k, r)$ , is given by the direct product of two groups  $G_c$  and  $G_a$ ;  $GR^*(2^k, r) \cong G_c \otimes G_a$ , where  $G_c$  is a cyclic group of order  $2^k - 1$  and  $G_a$  is an Abelian group of order  $2^{(k-1)r}$  whose structure is described below.

- If  $k \leq 2$ , then  $G_a$  is a direct product of  $r$  cyclic group each of order  $2^{k-1}$ .
- If  $k \geq 3$ , then  $G_a$  is a direct product of a cyclic group of order 2, a cyclic group of order  $2^{k-2}$ , and  $r-1$  cyclic groups each of order  $2^{k-1}$ .

Automorphisms of  $GR(p^k, r)$  [88]:

The group of automorphisms of  $GR(2^k, r)$  is a cyclic group of order  $r$ . They are given by

$$\sigma^j: \sum_{i=0}^{r-1} a_i x^i \longrightarrow \left( \sum_{i=0}^{r-1} a_i x^{2^{j*i}} \right) \bmod \psi(x), \quad 0 \leq j < r.$$

Examples:

$$GR(2^2, 3): \psi(x) = 3 + x + 2x^2 + x^3, \sigma^1(1) = \sigma^1(1), \sigma^1(x) = x^2, \sigma^1(x^2) = 2 + 3x + 3x^2.$$

$$GR(2^3, 3): \phi(x) = 7 + 5x + 6x^2 + x^3; \sigma^1(1) = \sigma^1(1), \sigma^1(x) = x^2, \sigma^1(x^2) = 2 + 7x + 3x^2.$$

$$GR(2^2, 4): \phi(x) = 1 + 3x + 2x^2 + x^4; \sigma^1(1) = \sigma^1(1), \sigma^1(x) = x^2, \sigma^1(x^2) = 3 + x + 2x^2, \\ \sigma^1(x^3) = 2 + 2x + x^2 + 3x^3.$$

Properties: (Proof in Appendix B)

A7.  $\sigma^i(ab) = \sigma^i(a)\sigma^i(b)$ , for any  $a, b \in GR(2^k, r)$  and for all  $i$ ,  $0 \leq i < r$ .

A8. If  $\sigma^i$ ,  $0 \leq i < rd$ , are the automorphisms of  $GR(2^k, rd)$  which fixes the ground ring  $Z_{2^k}$ , then  $\sigma^{rj}$ ,  $0 \leq j < d$ , are the automorphisms of  $GR(2^k, rd)$  which fixes the intermediate ring  $GR(2^k, r)$ .

These automorphisms are similar to the automorphisms of  $GF(2^r)$ . However they can be viewed in two different ways in case of  $GF(2^r)$ :

- (i) Vector space sense (VS): In  $GF(2^r)$ , field elements can be viewed as a vector space over  $GF(2)$  with  $1, x, x^2, \dots, x^{r-1}$  as the basis and automorphisms can be seen as linear transformation of the basis elements. The automorphism transformations are identical to the equations given above.
- (ii) Multiplicative sense (MS): Here multiplicative property of the elements of  $GF(2^r)$  is used to define automorphism mapping. For any  $\alpha \in GF(2^r)$ ,  $r$  automorphisms of  $GF(2^r)$  is defined as  $\sigma^i(\alpha) = (\alpha)^{2^i}; 0 \leq i < r$ .

Automorphisms defined above for  $GR(2^k, r)$  are similar to VS automorphisms of  $GF(2^r)$ . MS automorphism mappings of GF's will not carry over to the Galois rings. This is because the group of units of a Galois ring is in general Abelian group, whereas, in finite fields they form a cyclic group, and, hence in the later case, both VS and MS sense automorphisms are identical.

### Trace functions

Trace function maps elements of  $GR(2^k, r)$  to one of its intermediate sub rings. For every  $s$  that divides  $r$ , the trace function  $\text{tr}_s^r(\alpha)$  is a mapping from  $GR(2^k, r)$  to  $GR(2^k, s)$ ; and is given by

$$\text{tr}_s^r(\alpha) = \sum_{i=0}^{(r/s)-1} \sigma^{si}(\alpha), \text{ where } s \text{ divides } r.$$

Following properties can be easily verified (Proof in Appendix B).

- A9.  $\text{tr}_s^r(\alpha) = \text{tr}_s^r(\sigma^{sj}(\alpha))$  for all  $j$ , and belongs to the intermediate ring  $GR(2^k, s)$ .
- A10.  $\text{tr}_s^r(a\alpha + b\beta) = a\text{tr}_s^r(\alpha) + b\text{tr}_s^r(\beta)$  for all  $a, b \in GR(2^k, s)$  and  $\alpha, \beta \in GR(2^k, r)$
- A11. The equation  $\text{tr}_s^r(\alpha) = b$ , for any  $b$ , fixed element of  $GR(2^k, s)$  has exactly  $M^{r-s}$  solutions in  $GR(2^k, r)$ , where  $M = 2^k$ .
- A12.  $\text{tr}_1^r(\alpha) = \text{tr}_1^s(\text{tr}_s^r(\alpha))$

## Appendix B

### Properties of Automorphisms and Trace functions of $GR(2^k, r)$

Properties of Automorphisms:

B1.  $\sigma^i(ab) = \sigma^i(a)\sigma^i(b)$ , for any  $a, b \in GR(2^k, r)$  and for all  $i, 0 \leq i < r$ .

Proof: Let  $a = \sum_{j_1=0}^{r-1} a_{j_1} x^{j_1}$ , and  $b = \sum_{j_2=0}^{r-1} b_{j_2} x^{j_2} \in GR(2^k, r)$ , then

$$\sigma^i(ab) = \sum_{j_1=0}^{r-1} \sum_{j_2=0}^{r-1} a_{j_1} b_{j_2} x^{2^i(j_1+j_2)} \quad (\text{By Definition})$$

$$= \left( \sum_{j_1=0}^{r-1} a_{j_1} x^{2^i(j_1)} \right) \left( \sum_{j_2=0}^{r-1} b_{j_2} x^{2^i(j_2)} \right) \quad (\text{Rearranegemnt})$$

$$= \sigma^i(a)\sigma^i(b) \quad (\text{By Definition}) \quad \square$$

B2. If  $\sigma^i, 0 \leq i < rd$ , are the automorphisms of  $GR(2^k, rd)$  which fixes the ground ring  $Z_{2^k}$ , then  $\sigma^{rj}, 0 \leq j < d$ , are the automorphisms of  $GR(2^k, rd)$  which fixes the intermediate ring  $GR(2^k, r)$ .

Proof: It is easy to see that  $\sigma^{rj}, 0 \leq j < d$ , are automorphisms of  $GR(2^k, rd)$  and forms a cyclic group of order  $d$ . Then it is sufficient to show that these automorphisms leaves the elements of the subring  $GR(2^k, r)$  unaffected. Let  $\alpha$  be a primitive element in  $GR(2^k, rd)$  then  $\alpha^T, T = (2^{rd}-1)/(2^r-1)$  is primitive

in subring  $GR(2^k, r)$ . Then any element of  $GR(2^k, r)$  is of the form  $\sum_{i=0}^{r-1} a_i \alpha^{Ti}, a_i \in Z_{2^k}$ . Thus,

$$\sigma^{rj} \left( \sum_{i=0}^{r-1} a_i \alpha^{Ti} \right) = \sum_{i=0}^{r-1} a_i \alpha^{2^{rj}(Ti)} = \sum_{i=0}^{r-1} a_i \alpha^{2^{(Tij)}} \text{, since } ((2^r-1)+1)2^j((2^{rd}-1)/(2^r-1))i = p^{j(Ti)} \pmod{(2^{rd}-1)}, \text{ and}$$

hence belongs to the subring  $GR(2^k, r)$ .  $\square$

## Properties of Trace functions

B3.  $\text{tr}_s^r(\alpha) = \text{tr}_s^r(\sigma^{sj}(\alpha))$  for all  $j$ , and belongs to intermediate ring  $\text{GR}(2^k, s)$ .

$$\begin{aligned}
 \text{Proof: } \text{tr}_s^r(\sigma^{sj}(\alpha)) &= \sum_{i=0}^{(r/s)-1} \sigma^{si}(\sigma^{sj}(\alpha)) && \text{By Definition} \\
 &= \sum_{i=0}^{(r/s)-1} \sigma^{s(i+j)}(\alpha) && \text{(From A?)} \\
 &= \sum_{i=0}^{(r/s)-1} \sigma^{si}(\alpha) && \text{(Rearrangement)} \\
 &= \text{tr}_s^r(\alpha) && \text{(By Definition)}
 \end{aligned}$$

Also,  $\sigma^{sj}(\text{tr}_s^r(\alpha)) = \text{tr}_s^r(\alpha)$ ,  $0 \leq j < r/s$ , and hence  $\text{tr}_s^r(\alpha)$  belongs to the intermediated ring  $\text{GR}(2^k, s)$ .  $\square$

B4.  $\text{tr}_s^r(a\alpha + b\beta) = a\text{tr}_s^r(\alpha) + b\text{tr}_s^r(\beta)$  for all  $a, b \in \text{GR}(2^k, s)$  and  $\alpha, \beta \in \text{GR}(2^k, r)$

$$\begin{aligned}
 \text{Proof: } \text{tr}_s^r(a\alpha + b\beta) &= \sum_{i=0}^{(r/s)-1} \sigma^{si}(a\alpha + b\beta) && \text{(By Definition)} \\
 &= a \left( \sum_{i=0}^{(r/s)-1} \sigma^{si}(\alpha) \right) + b \left( \sum_{i=0}^{(r/s)-1} \sigma^{si}(\beta) \right) && \text{(From (B.1) and (B.2) and linearity)} \\
 &= a\text{tr}_s^r(\alpha) + b\text{tr}_s^r(\beta) && \text{(By Definition)} \quad \square
 \end{aligned}$$

B5. The equation  $\text{tr}_s^r(\alpha) = b$ , for any  $b$ , fixed element of  $\text{GR}(2^k, s)$  has exactly  $M^{r-s}$  solutions in  $\text{GR}(2^k, r)$ , where  $M = p^k$ .

Proof: From the properties A.1 and A.2,  $\text{tr}_s^r(\alpha) \in \text{GR}(2^k, s)$ , for all  $\alpha \in \text{GR}(2^k, r)$ , and hence  $\text{tr}_s^r(\cdot)$  is a linear transformation from  $\text{GR}(2^k, r)$  to  $\text{GR}(2^k, s)$ . To prove that this mapping is onto, it is suffice to show the existence of  $\alpha \in \text{GR}(2^k, r)$  such that  $\text{tr}_s^r(\alpha) = a \in \text{GR}^*(2^k, s)$ , a unit. Such an  $\alpha$  always exists due to Dadekind's theorem for local rings (Given at the end of the Appendix). Let  $H(\text{tr}^{-1}(b))$ ,  $b \in \text{GR}(2^k, s)$  be a collection of  $\text{GR}(2^k, r)$  elements whose trace is  $b$ . Note that  $H(\text{tr}^{-1}(b))$  always exists since trace is an onto linear mappping. We note that the cardinalities of all the sets  $H(\text{tr}^{-1}(b))$ ,  $b \in \text{GR}(2^k, r)$ , are equal, as for any non zero element  $b \in \text{GR}(2^k, s)$ ,  $H(\text{tr}^{-1}(b))$  is formed by multiplying  $(a^{-1}b)$  to all the elements of  $H(\text{tr}^{-1}(a))$ . ( $a^{-1}$  exists, since there exists  $\alpha$  such that  $\text{tr}_s^r(\alpha) = a$ ,  $a$ : unit). There are precisely  $M^s$  such sets accounting for  $M^r$  elements of  $\text{GR}(2^k, r)$ ,  $M = p^k$ . Thus cardinality of each subgroup is  $M^{r-s}$ .  $\square$

$$\text{B.6. } \text{tr}_1^r(\alpha) = \text{tr}_1^s(\text{tr}_s^r(\alpha))$$

$$\begin{aligned} \text{Proof: RHS} &= \text{tr}_1^s\left(\sum_{i=0}^{(r/s)-1} \sigma^{si}(\alpha)\right) && (\text{By Definition}) \\ &= \sum_{j=0}^{s-1} \sigma^j\left(\sum_{i=0}^{(r/s)-1} \sigma^{si}(\alpha)\right) && (\text{Re arrangement}) \\ &= \sum_{j=0}^{r-1} \sigma^j(\alpha) = \text{LHS} && (\text{By Definition}) \quad \square \end{aligned}$$

### Dedekind's Theorem for Finite Local rings.

**Theorem B.1:** If  $R$  is a finite local commutative ring and  $\sigma^1, \dots, \sigma^n$  are distinct cyclic automorphisms of  $R$ , it is not possible to find  $a_1, a_2, \dots, a_n$  not all zero such that

$$a_1 \sigma^1(u) + a_2 \sigma^2(u) + \dots + a_n \sigma^n(u) = 0 \quad (\text{B.1})$$

and also it is not possible to find  $a_1, a_2, \dots, a_n$  not all zero divisors such that

$$a_1 \sigma^1(u) + a_2 \sigma^2(u) + \dots + a_n \sigma^n(u) = R_I \quad (\text{B.2})$$

where  $R_I$  is any ideal of zero divisors present in  $R$ .

**Proof:** The proof of the theorem runs similar to its counterpart for finite fields [94]. Suppose we find set of  $a_i$ 's satisfying (B.1), then we could find such a relation having as few nonzero terms as possible; on renumbering the following minimal relation can be assumed:

$$a_1 \sigma^1(u) + a_2 \sigma^2(u) + \dots + a_m \sigma^m(u) = 0 \quad (\text{B.3})$$

where  $a_1, \dots, a_m$  are all different from zero. We may assume  $m > 1$ , since if  $m = 1$ ,  $a_1 \sigma^1(u) = 0$ , for all  $u \in R$ , implies  $a_1 = 0$ . Since the automorphisms are distinct, there exists a unit element  $c \in R$ , such that  $\sigma^1(c) \neq \sigma^m(c)$ . The relation (B.3) must hold for  $(cu)$  also, since for all  $u \in R$ ,  $cu \in R$ . Thus, applying  $cu$  in (B.3), we have

$$a_1 \sigma^1(c) \sigma^1(u) + a_2 \sigma^2(c) \sigma^2(u) + \dots + a_m \sigma^m(c) \sigma^m(u) = 0 \quad (\text{B.4}).$$

But, (B.3) \*  $\sigma^1(c) -$  (B.4) becomes

$$b_2 \sigma^2(u) + \dots + b_m \sigma^m(u) = 0 \quad (\text{B.5})$$

where  $b_i = a_i(\sigma^i(c) - \sigma^1(c))$  for  $i = 2, \dots, m$ . Observe that  $b_i$ 's are in  $R$ , and  $b_m \neq 0$ , since  $a_m \neq 0$  and  $\sigma^1(c) \neq \sigma^m(c)$ ; yet (B.5) is true. This produces a shorter relation than (B.3) resulting in a contradiction. Hence the first assertion. To prove the second, suppose that we find such a relation, then multiplying (B.2) with the annihilator ideal of  $R_I$  yields the relation of the type (B.1). Not all the coefficients in this relation are zeroes, since in the original equation not all coefficients are zero divisors. Thus, this contradicts the first assertion. Hence the proof.  $\square$ .

# Appendix C

## Irreducible polynomials over $Z_4$ and $Z_8$

- Note: 1. Irreducible polynomials of degree  $r$  are listed as vectors of length  $r+1$ ; for example 3121 means a polynomial  $3+x+2x^2+x^3$
2. Exponent of a polynomial  $a(x)$  is the least integer  $i$  such that  $a(x)$  divides  $x^i-1$ .

### C1 All Basic Monic Irreducible Polynomials over $Z_4$ of degree $r$ ; $r = 3$ and 4

$r = 3$

Polynomial	Exponent	Polynomial	Exponent
3121	7	3231	7
1121	14	1211	14
3321	14	3031	14
1321	14	1011	14
3101	14	3011	14
1101	14	1031	14
3301	14	3211	14
1301	14	1231	14

$r = 4$

Polynomial	Exponent	Polynomial	Exponent
13201	15	11111	5
10231	15	11201	30
13131	10	10211	30
13001	30	13311	10
12231	30	11001	30
11331	10	12211	30
13221	30	13111	10
10011	30	11221	30
11131	10	10031	30
13021	30	11311	10
12011	30	11021	30
13331	10	12031	30
31201	30	33131	10
32231	30	33201	30
31111	10	32211	30
31001	30	31331	10
30231	30	33001	30
33311	10	30211	30
31221	30	31131	10
32011	30	33221	30
33111	10	32031	30
31021	30	33331	10
30011	30	33021	30
31311	10	30031	30

C2 All Basic Monic Irreducible Polynomials over  $Z_8$  of degree  $r$ ;  $r = 3$ 

Polynomial	Exponent	Polynomial	Exponent	Polynomial	Exponent
7561	7	7231	7	5521	14
5211	14	3561	14	3271	14
1521	14	1251	14	7721	28
7471	28	5361	28	5051	28
3721	28	3431	28	1361	28
1011	28	7161	14	7631	14
5121	14	5611	14	3161	14
3671	14	1121	14	1651	14
7321	28	7071	28	5761	28
5451	28	3321	28	3031	28
1761	28	1411	28	7541	28
7011	28	5501	28	5471	28
3541	28	3051	28	1501	28
1431	28	3301	28	3251	28
1741	28	1231	28	7301	28
7211	28	5741	28	5271	28
7141	28	7411	28	5101	28
5071	28	3141	28	3451	28
1101	28	1031	28	3701	28
3651	28	1341	28	1631	28
7701	28	7611	28	5341	28
5671	28	7521	14	7671	14
5561	14	5651	14	3521	14
3631	14	1561	14	1611	14
7761	28	7031	28	5321	28
5411	28	3761	28	3071	28
1321	28	1451	28	7121	14
7271	14	5161	14	5251	14
3121	14	3231	14	1161	14
1211	14	7361	28	7431	28
5721	28	5011	28	3361	28
3471	28	1721	28	1051	28
7501	28	7451	28	5541	28
5031	28	3501	28	3411	28
1541	28	1071	28	3341	28
3611	28	1701	28	1671	28
7341	28	7651	28	5701	28
5631	28	7101	28	7051	28
5141	28	5431	28	3101	28
3011	28	1141	28	1471	28
3741	28	3211	28	1301	28
1271	28	7741	28	7251	28
5301	28	5231	28		

C3 Basic Irreducible Polynomials over  $Z_4$  of Degree  $r$ ;  $r = 5, 6, 7, 8, 9$   
 Such that Exponent Divides  $2^r - 1$

$r = 5$

Polynomial	Exponent	Polynomial	Exponent
323001	31	321311	31
331031	31	331321	31
310311	31	300121	31

$r = 6$

Polynomial	Exponent	Polynomial	Exponent
1302001	63	1130321	21
1110231	63	1001001	9
1211031	63	1301121	63
1230311	21	1320111	63
1002031	63		

$r = 7$

Polynomial	Exponent	Polynomial	Exponent
31002001	127	31230321	127
33112201	127	32113111	127
30211321	127	30010201	127
32322111	127	33313321	127
33112311	127	31232231	127
33322121	127	33123311	127
30203001	127	32101231	127
31221231	127	30223311	127
32133201	127	30020031	127



C3 continued...

 $r = 8$ 

Polynomial	Exponent	Polynomial	Exponent
123132201	255	113213321	85
132011111	51	100103121	255
123113031	85	111021311	255
132103001	255	113030311	17
121201121	255	132302031	85
130023121	255	130330201	51
111311201	85	121320031	255
121301001	255	111310321	255
102113111	85	130200111	255
102313201	17	100301231	255
111002031	255	102033031	51
121102121	255	113120111	255
123312311	85	130203231	85
123013111	255	111110231	51
130311321	85	102231321	255

 $r = 9$ 

Polynomial	Exponent	Polynomial	Exponent
3020300001	511	3023321001	511
3020112231	511	3021322121	73
3120122031	511	3231212201	511
3312113201	511	3002213031	511
3103121121	511	3230220111	511
3312320001	73	3003033111	511
3100031111	511	3311022111	511
3121031031	511	3101322001	511
3000200031	73	3311031201	511
3233001311	511	3120111031	511
3123001311	511	3211331201	511
3103103231	511	3210301311	511
3212300121	511	3213130321	511
3210131321	511	3313001121	511
3331101001	511	3232213201	73
3101131111	511	3003201231	73
3332203311	511	3212122031	511
3310132321	511	3230012321	511
3123021001	73	3023113321	511
3021332311	511	3313010321	511
3102232321	511	3333133031	511
3333100031	511	3313001231	511
3100020001	73	3330220121	511
3022323121	511	3003211201	511
3212130311	511	3000212311	73
3103330231	511	3023103311	511
3122330201	511	3102230231	511
3233231031	511	3000010201	511

## Appendix D

### Properties of $P_p^n[w(\xi)]$ and $PGR(V^k, r)$ [25, 88, 95,]

**Definition D.1:** Residue class polynomial ring  $P_p^n[w(\xi)]$  or simply  $P_p^n[w]$ : Let  $GF(p)[\xi]$  be the ring of all polynomials over  $GF(p)$ , the Galois field with  $p$  elements,  $p$ : prime. Let  $w(\xi)$  be a polynomial of degree  $n$  over  $GF(p)$ . Then  $P_p^n[w(\xi)]$  is defined as  $GF(p)[x]/w(\xi)$ , the residue class polynomial ring  $GF(p)[x] \bmod w(\xi)$  ( Set of all polynomials over  $GF(p)$  of degree  $< n$ ). While representing  $P_p^n[w]$  ring elements, the indeterminate  $\xi$  may be dropped for convinience.

D1: [25,95]  $P_p^n[w]$  is a vector space of dimension  $n$  over  $GF(p)$ .

D2:  $P_p^n[w]$  is a commutative algebra over  $GF(p)$ . It is also called as polynomial algebra generated a polynomial  $w(\xi)$ .

**Classification of  $P_p^n[w(\xi)]$ :** It is classified in to local or semi local ring depending on the nature of  $w(\xi)$ . If  $w(\xi)$  is a power of an irreducible polynomial  $a(\xi)$  over  $GF(p)$ ,  $w(\xi) = a(\xi)^k$ ,  $k$ :positive integer, then  $P_p^n[w(\xi)]$  is a local ring; and when  $k = 1$ , it is  $GF(p^n)$ . If  $w(\xi)$  is a composite polynomial, then  $P_p^n[w(\xi)]$  is a semi local ring.

D3:  $P_p^n[w(\xi)]$  is expressed as direct sum of its local constituents by making use of Chinese reminder theorem (CRT) for polynomials.

If  $w(\xi) = \prod_{i=1}^r (w_i(\xi))^{k_i}$ , then

$$P_p^n[w(\xi)] = P_p^{m_1 k_1}[w_1^{k_1}] \oplus \dots \oplus P_p^{m_i k_i}[w_i^{k_i}] \oplus \dots \oplus P_p^{m_r k_r}[w_r^{k_r}], \quad (D.1)$$

where  $\oplus$  represents direct sum notation for rings,  $m_i$  is the degree of  $w_i$ ,  $k_i \geq 1$ .

A local residue class polynomial ring  $P_p^n[w^k(a)]$ ,  $w(\xi)$  is irreducible over  $GF(p)$ ,  $\deg(w(\xi)) = m$ ,  $k > 1$ ,  $n = mk$ , is, in short, denoted by  $P_p^n[w^k]$ .

Properties of the ring  $P_p^n[w^k]$ : This is a local ring with chain of ideals generated by  $\langle w(\xi)^j \rangle$ ,  $0 \leq j \leq k$ , with  $\langle w(\xi)^{j_1} \rangle \subset \langle w(\xi)^{j_2} \rangle$ ,  $j_1 \leq j_2$ . The ideal  $\langle w(\xi) \rangle$  is the maximal ideal. The natural projection from  $P_p^n[w^k]$  to the residue field  $P_p^m[w]$  is denoted by  $\mu^k$ . In fact there are  $k$  such projections from  $P_p^n[w^k]$  to  $P_p^{mj}[w^j]$ ,  $0 \leq j < k$ .

Zero divisors of  $P_p^n[w^k]$ :

D4: Elements of the maximal ideal,  $\langle a(x) \rangle$  gives all the zero divisors of the ring. Every ideal of  $P_p^n[w^k]$  is generated by an element  $w(\xi)^i$ ,  $0 \leq i \leq k$  and is of the form

$$\langle w(\xi)^i \rangle = w(\xi)^i P_p^n[w^k] \quad 0 \leq i \leq k. \quad (D.2)$$

Thus the number of zero divisors is equal to  $p^{m(k-1)}$ .

Group of units of  $P_p^n[w^k]$  [88,95]:  $P_p^n[w^k]^*$ :

D5  $P_p^n[w^k]^*$  is given by the direct product of two groups  $G_{\text{PRC}}$  and  $G_{\text{PRA}}$ :

$$P_p^n[w^k] = G_{\text{PRC}} \otimes G_{\text{PRA}}, \quad (D.3)$$

where  $G_{\text{PRC}}$  is a cyclic group of order  $p^m - 1$  and  $G_{\text{PRA}}$  is an Abelian group of order  $p^{(k-1)m}$ .

**Lemma D.1:** The set  $\{G_{\text{PRC}}, 0\}$  is isomorphic to residue field  $P_p^m[w]$  and also a subspace of  $P_p^n[w^k]$  and hence it is a subring over  $P_p^n[w^k]$ .

**Proof:** Since  $G_{\text{PRC}}$  is a cyclic group of order  $p^m - 1$ , the set  $\{G_{\text{PRC}}, 0\}$  satisfies multiplicative axiom of the field. It is sufficient to show that the set is closed under addition. Let  $\alpha_1, \alpha_2 \in G_{\text{PRC}}$ , then

$$(\alpha_1 + \alpha_2)^{p^m} = (\alpha_1^{p^m} + \alpha_2^{p^m}) = (\alpha_1 + \alpha_2)$$

since for any ring of characteristic  $p$ ,  $(a + b)^p = (a^p + b^p)$ . This implies that  $(\alpha_1 + \alpha_2)^{p^m - 1} = 1$ , and  $(\alpha_1 + \alpha_2) \in G_{\text{PRC}}$ . Hence the set  $\{G_{\text{PRC}}, 0\}$  is closed under addition and the proof is done.  $\square$

**Remark D.1:** The set  $\{G_{\text{PRC}}, 0\}$  is not an ideal but a subspace of  $P_p^n[w^k]$ . It is referred as  $SP_p^m[w]$ .

**Example:** The ring  $P_2^6[(1 + \xi + \xi^3)^2]$ ,  $w(\xi) = 1 + \xi^2 + \xi^6$ .

**Zero Divisors:**  $\{0, (1 + \xi + \xi^3), (1 + \xi + \xi^3)\alpha, \dots, (1 + \xi + \xi^3)\alpha^7\}$ , where  $\alpha$  is primitive in  $G_{\text{PRC}}$ ;  $\alpha = \xi^2$ .  $G_{\text{PRC}}$  is the subfield  $SP_2^3[w]$ . The basis elements of  $SP_2^3[(1 + \xi + \xi^3)]$  are given by  $\{1, \xi^2, \xi^4\}$

## Properties of $\text{PGR}(V^k, r)$ :

**Definition D.2:** Galois extension ring  $\text{PGR}(V^k, r)$ : Let  $P_p^n[w^k][x]$  be the ring of all polynomials over  $P_p^n[w^k]$ . Let  $\psi(x)$  be a basic monic irreducible polynomial of degree  $r$  over  $P_p^n[w^k]$ .  $\text{PGR}(V^k, r)$  is defined as  $P_p^n[w^k][x]/\psi(x)$ , the residue class polynomial ring  $P_p^n[w^k][x]$  modulo  $\psi(x)$  (set of all polynomials of degree  $r-1$  over  $P_p^n[w^k]$ ).

## Construction of $\text{PGR}(V^k, r)$ :

Choose  $\psi(x)$ , a basic monic irreducible polynomial over  $P_p^n[w^k]$  such that the multiplicative order of element  $x$  in  $P_p^n[w^k][x]/\psi(x)$  divides  $(x^{V^r-1}-1)$ . Construction of such a polynomial is given below. Then  $\text{PGR}(V^k, r)$  contains elements of the form  $\sum_{i=0}^{r-1} a_i x^i$ ,  $a_i \in P_p^n[w^k]$ . Alternatively elements of  $\text{PGR}(V^k, r)$  can be viewed as vectors of length  $r$  over  $P_p^n[w^k]$ .

*Construction of irreducible polynomial over  $P_p^n[w^k]$ :* A basic monic irreducible polynomial over  $P_p^n[w^k]$  is constructed from an irreducible polynomial over  $\text{GF}(V)$  as follows. Let  $f$  be the isomorphic mapping from  $\text{GF}(V)$  to  $\text{SP}_p^m[w]$  which is a subfield of  $P_p^n[w^k]$  and let  $\psi^1(x)$  be an primitive irreducible polynomial of degree  $r$  over  $\text{GF}(V)$ . Then mapping the coefficients  $\psi^1(x)$  by the mapping  $f$  gives an irreducible polynomial over  $P_p^n[w^k]$ ;  $\psi(x) = f(\psi^1(x))$ . Multiplicative order of element  $x$  in  $P_p^n[w^k][x]/\psi(x)$  divides  $(x^{V^r-1}-1)$  since  $\psi(x)$  is primitive.

*Example D.2:* Irreducible polynomial over  $P_2^4[(1+\xi+\xi^2)^2]$ : Polynomial  $\beta + \beta^2 x + x^2 + x^3$  is a primitive irreducible over  $\text{GF}(2^2)$  where  $\beta^3 = 1$ ,  $\beta^2 = \beta + 1$ . In this case the set  $\{0, 1, \xi^2 = \beta, 1 + \xi^2 = \beta^2\}$  is the subfield  $\text{SP}_2^2[1 + \xi + \xi^2]$  isomorphic to  $\text{GF}(4)$ . Then a mapping from  $\delta \rightarrow \xi^2$ , applied on the coefficients yields a corresponding irreducible polynomial over  $P_2^4[(1 + \xi + \xi^2)^2]$ . Thus  $\xi^2 + (1 + \xi^2)x + x^2 + x^3$  is a primitive irreducible polynomial over  $P_2^4[(1 + \xi + \xi^2)^2]$ . Hence the set of elements  $\{(a_0 + a_1 x + \dots + a_2 x^{r-1}), a_i \in \text{SP}_2^2[1 + \xi + \xi^2]\}$  is isomorphic to  $\text{GF}(4^3)$ . Similarly polynomial  $\xi^4 + (1 + \xi^4)x + x^2 + x^3$  is a monic basic primitive irreducible over  $P_2^6[(1 + \xi + \xi^2)^3]$ .

$\text{PGR}(V^k, r)$  is unique for a given  $r$ , degree of the extension [McDon]. Also it is clear that  $\text{PGR}(V^k, r)$  is a module over  $P_p^n[w^k]$ . But  $P_p^n[w^k]$ , a local ring can also be viewed as a vector space. When  $r = 1$ ,  $\text{PGR}(V^k, r)$  is equal to  $P_p^n[w^k]$  and when  $k = 1$  it is isomorphic to  $\text{GF}(V^r)$ .

Following two mappings are similar to  $GR(p^k, r)$  [88].

D6: For every positive integer  $d$ , there is a natural inclusion of  $PGR(V^k, r)$  into  $PGR(V^k, dr)$ , similar to galois fields. In other words, every sub ring of  $PGR(V^k, r)$  is of the form  $PGR(V^k, s)$  for some divisor  $s$  of  $r$ . Conversely, for every positive divisor  $s$  of  $r$  there is a unique sub ring  $R$  which is isomorphic to  $PGR(V^k, s)$ .

D7: There is a natural homomorphic mapping  $(\mu^i)$  from  $PGR(V^k, r)$  to  $PGR(V^k, r)$ , for each  $i$ ,  $0 \leq i < k$ , and there are exactly  $r$  such mappings.

Ideal structure of  $PGR(V^k, r)$ :

D8: Every ideal in  $PGR(V^k, r)$  is principal, generated by an element of the type  $w(\xi)^j$ ,  $0 \leq j \leq k$  and is given by  $\langle w(\xi)^j PGR(V^k, r) \rangle$ ,  $0 \leq j \leq k$ . The ideals exhibit the chain property such that  $\langle w^k PGR(V^k, r) \rangle \subset \langle w^{k-1} PGR(V^k, r) \rangle \subset \dots \subset \langle w PGR(V^k, r) \rangle \subset \langle PGR(V^k, r) \rangle$

D.9: Ideal  $\langle w^j \rangle$ ,  $0 \leq j \leq k$  is isomorphic to  $PGR(V^{k-j}, r)$ .

D.10: The extension field of subring  $SP_p^m[w]$  is the subfield isomorphic to  $GF(V^r)$  (set of polynomials of degree less than  $r$  with coefficients from  $SP_p^m[w]$ ). We shall refer this as  $SPGR(V, r)$ .

D.11: Every non-zero element of  $PGR(V^k, r)$  may be written as  $uw^t$ , where  $u$  is a unit and  $t$  an integer  $0 \leq t \leq k$ . In such a representation  $t$  is unique and  $u$  is unique modulo  $w^{k-t}$ .

D.11: Zero divisors of  $PGR(V^k, r)$ : The elements of the maximal ideal  $\langle w \rangle$  gives all the zero divisors and the total number of zero divisors is equal to  $V^{(k-1)r}$ .

Group of units of  $PGR(V^k, r)$ :  $PGR^*(V^k, r)$ :

D12:  $PGR^*(V^k, r)$  is given by the direct product of two groups  $G_c$  and  $G_a$ ,

$$PGR^*(V^k, r) \cong G_c \otimes G_a \quad (D.4)$$

where  $G_c$  is cyclic group of order  $V^r - 1$  and  $G_a$  is an Abelian group of order  $V^{(k-1)r}$ . Elements  $G_a \in PGR(V^k, r)$  are given by the set

$$\{1 + w(A'), A' \text{ takes all the values of } \mu PGR(V^k, r) \cong PGR(V^{k-1}, r)\} \quad (D.5)$$

On the lines of proof of Lemma D.1, the set  $\{G_{c,0}\}$  can be shown to be a subfield of  $PGR(V^k, r)$ ; it is denoted by  $SPGR(V, r) = GF(V^r)$ .

### Automorphisms of $PGR(V^k, r)$ [88]:

The group of automorphisms of  $GR(p^k, r)$  is a cyclic group of order  $r$ . They are given by

$$\sigma^j: \sum_{i=0}^{r-1} \alpha_i x^i \longrightarrow \left( \sum_{i=0}^{r-1} \alpha_i x^{V^{j \cdot i}} \right) \bmod \psi(x), \quad 0 \leq j < r. \quad (D.6)$$

### Properties of Automorphisms

D13:  $\sigma^i(ab) = \sigma^i(a)\sigma^i(b)$ , for any  $a, b \in$  and for all  $i$ ,  $0 \leq i < r$ .

D14: If  $\sigma^i$ ,  $0 \leq i < rd$ , are the automorphisms of  $PGR(V^k, rd)$ , then  $\sigma^{di}$ ,  $0 \leq i \leq r$  are the automorphisms of  $PGR(V^k, r)$ .

### Trace functions:

Trace function maps elements of  $PGR(V^k, r)$  to its intermediate sub rings. It is denoted by  $tr_s^r(\alpha)$ ,  $s$  divides  $r$ , a mapping from  $PGR(V^k, r)$  to  $PGR(V^k, s)$  and is given by

$$tr_s^r(\alpha) = \sum_{i=0}^{(r/s)-1} \sigma^{si}(\alpha) \quad \text{where } s \text{ divides } r. \quad (D.7)$$

Following properties can be easily verified.

D15:  $tr_s^r(\alpha) = tr_s^r(\sigma^{si}(\alpha))$  for all  $i$

D16:  $tr_s^r(a\alpha + b\beta) = a tr_s^r(\alpha) + b tr_s^r(\beta)$  for all  $a, b \in PGR(V^k, s)$  and  $\alpha, \beta \in PGR(V^k, r)$

D17: The equation  $tr_s^r(\alpha) = b$ , for any  $b$ , fixed element of  $PGR(V^k, s)$  has exactly  $M^{r-s}$  solutions in  $PGR(V^k, r)$ , where  $M = V^k$ .

D18:  $tr_1^r(\alpha) = tr_1^s(tr_s^r(\alpha))$

D13 to D18 can be proved using similar arguments as done with their counterparts in Appendix A concerning properties of automorphism and trace functions of  $GR(2^k, r)$ .

## Appendix E

### Sequence Sets satisfying Welch's Bound with Equality [41]

Let  $X = \{x_m, m = 1, \dots, M\}$  be a set of  $M$  complex vectors of length  $L$ . Then the inner-product between the vectors  $x_m$  and  $x_n$  is given by

$$C_{mn}(0) = \sum_{i=1}^L (x_{mi} x_{ni}^*). \quad (E.1)$$

The energy of the vector  $x_m$  is defined as

$$E = \sum_{i=1}^L (x_{mi} x_{mi}^*). \quad (E.2)$$

**Lemma E.1:** For any real numbers  $a_1, a_2, \dots, a_L$ ,

$$\sum_{i=1}^L (a_i)^2 \geq \frac{1}{L} \left[ \sum_{i=1}^L a_i \right]^2. \quad (E.3)$$

The equality holds if and only if  $a_1 = a_2 = \dots = a_L$ .

**Proof:** Choose  $A = [a_1, a_2, \dots, a_L]$  and  $B = (1/L)[1, 1, \dots, 1]$ , vectors of length  $L$ . Then proof follows from Cauchy-Schwarz inequality which states that

$$C_{AA}(0)C_{BB}(0) \geq (C_{AB}(0))^2$$

with equality if and only if  $A$  and  $B$  are proportional.  $\square$

**Welch's Bound Theorem:** If  $x_1, x_2, \dots, x_M$  are vectors of energy  $E$  in  $C^L$ , then a sum of inner-products satisfy

$$\sum_{n=1}^M \sum_{m=1}^M |C_{mn}(0)|^2 \geq \frac{(M E)^2}{L}, \quad (E.4)$$

where  $|x|$  means modulus value of  $x$ . Equality holds in the above equation, if and only if, in an  $M$  by  $L$  array having  $x_1, x_2, \dots, x_M$  as rows, the columns are mutually orthogonal and all columns have same energy.

Proof:

$$\begin{aligned}
 \sum_{m=1}^M \sum_{n=1}^M |C_{mn}(0)|^2 &= \sum_{m=1}^M \sum_{n=1}^M \left| \sum_{i=1}^L (x_{mi} x_{ni}^*) \right|^2 && \text{(From Definition)} \\
 &= \sum_{m=1}^M \sum_{n=1}^M \left( \sum_{i=1}^L (x_{mi} x_{ni}^*) \right) \left( \sum_{j=1}^L (x_{mj}^* x_{nj}) \right) && \text{(Rearranging)} \\
 &= \sum_{i=1}^L \sum_{j=1}^L \left( \sum_{m=1}^M (x_{mi} x_{mj}^*) \right) \left( \sum_{n=1}^M (x_{ni}^* x_{nj}) \right) && \text{(Reordering)}
 \end{aligned} \tag{E.5}$$

Consider the  $M$  by  $L$  array  $A$  having  $x_1, x_2, \dots, x_M$  as rows. Let  $A^i$  denote  $i^{\text{th}}$  column of this array;  $A^i = (x_{1i}, x_{2i}, \dots, x_{Mi})^T$ , where  $T$  represents transpose operation. Let  $C^{ij}$  denote inner-product between  $A^i$  and  $A^j$ ;  $C^{ij} = \sum_{m=1}^M (x_{mi} x_{mj}^*)$ . Then we can rewrite (E.5) as

$$\sum_{m=1}^M \sum_{n=1}^M |C_{mn}(0)|^2 = \sum_{i=1}^L \sum_{j=1}^L |C^{ij}|^2 \tag{E.6}$$

Retaining only the terms which for which  $i = j$ , (E.6) can be bounded by

$$\sum_{m=1}^M \sum_{n=1}^M |C_{mn}(0)|^2 \geq \sum_{i=1}^L |C^{ii}|^2 \tag{E.7}$$

For the bound (E.7) to be equality if and only if  $C^{ij} = 0$  whenever  $i \neq j$  or, equivalently, if and only if the columns of  $A$  are mutually orthogonal. Now Lemma A.1 can be used to lowerbound the RHS of (E.7), thus we have

$$\sum_{m=1}^M \sum_{n=1}^M |C_{mn}(0)|^2 \geq \frac{1}{L} \left( \sum_{i=1}^L |C^{ii}| \right)^2 \tag{E.8}$$

Since  $C^{ii}$  is the energy of the  $i^{\text{th}}$  column, from Lemma E.1, the bound (E.8) is an equality if and only if equality holds in (E.7) and columns of  $A$  have the same energy. The total energy of the terms in  $A$  can be written as

$$\sum_{i=1}^L |C^{ii}| = \sum_{m=1}^M |C_{mm}(0)| = M E \tag{E.9}$$

since, by hypothesis, each of the  $M$  rows of  $A$  has energy  $E$ . Then using this equation in (E.8) gives Welch's bound.  $\square$



## REFERENCES

1. D. Sarwate and M. Pursley, "Crosscorrelation Properties of Pseudo random and Related Sequences", Proceedings of the IEEE, May 1980, p 593-619.
2. A. Lempel and H. Greenberger, "Families of Sequences with Optimal Hamming Correlation Properties", IEEE Trans. Inform. Theory, IT-20, No. 1. Jan. 1974, pp 90-94.
3. S.M. Krone and D.V. Sarwate, "Quadriphase Sequences for Spread-Spectrum Multiple-Access Communication", Vol. IT-30, No. 3, May 1984, pp 520-529.
4. F.J. MacWilliams and N.J.A. Sloane, "Pseudo-Random Sequences and Arrays" Proceedings of the IEEE, Vol. 64, No. 12, Dec. 1976, pp 1715-1729.
5. M.K. Simon, J. K. Omura, R. A. Scholtz and B. K. Levit, "Spread Spectrum Communications", Vol. 1, Computer Science Press, 1985.
6. M.B. Pursley, "Spread Spectrum Multiple-Access Communications Multiuser Communication Systems", in Multi-User Communication systems, G.Longo, Ed., CISM Lecture Notes No. 265, Vienna and New York: Springer Verlag, 1981, pp 139-199.
7. S.A. Fredricsson, "Pseudo-Randomness Properties of Binary Shift Register Sequences", IEEE Trans. Inform. Theory, IT-21, Jan. 1975, pp- 115-120.
8. M.B. Pursley and D.V. Sarwate, "Evaluation of Correlation Parameters for Periodic Sequences", IEEE Trans. Inform. Theory, IT-23, Jul. 1977, pp 508-513.
9. D.V. Sarwate, "An Upper Bound on the Aperiodic Autocorrelation Function for a Maximal Length Sequence", IEEE Trans. Inform. Theory, IT-30, Jul. 1984, pp 685-687.
10. M.J.E Golay, "Sieves for Low Autocorrelation Binary sequences", IEEE Trans. Inform. Theory, IT-23, Jan. 1977, pp 43-51.
11. W.O. Alltop, "Complex Sequences with Periodic Correlations", IEEE Trans. Inform. Theory, IT-26, May 1980, pp 350-354.
12. M.B. Pursley and H.F.A. Roefs, "Numerical Evaluation of Correlation Parameters for Optimal Phases of Binary Shift-Register Sequences", IEEE Trans. on Communications, COM-27, Oct. 1979, pp 1597-1604.
13. K.S. Schneider and R. S. Orr, "Aperiodic Correlation Constraints on Large Binary Sequence Sets, IEEE Trans. Inform. Theory, IT-21, Jan 1975, pp 79-84.
14. D.V. Sarwate, "Mean-Square Correlation of Shift-register Sequences", IEE Proceedings, Vol. 131, Part F, No. 2, April 1984, pp 101-106.
15. P.S. Moharir and A. Selvarajan, "Sequences with Good Autocorelation for Pulse Compression and Synchronization" Technical report :CIP/QIP/1.1, Electrical Communication Department, I.I.Sc, Bangalore, January 1974.
16. R. Turyn, "Sequences with Small Correlation", in Error Correcting Codes, H.B. Mann, Ed. New York: Wiley, 1968.
17. A. Milewski, "Periodic Sequences with Optimal Properties for Channel Estimation and Fast Start-Up Equalization", IBM J. RES. DEVELOP., Vol.-27, No. 5, Sept. 1983, pp 426-431.
18. M.J.E Golay, "A Class of Finite Binary Sequences with Alternate Autocorrelation Values Equal to Zero", IEEE Trans. Inform. Theory, Vol IT-18, No. 3, May 1972, pp 449-450.

19. S. W. Golomb, Shift Register Sequences, Holden-Day, San Francisco, 1967.
20. C. Ronse, "Feedback Shift Registers", Lect. Not. Comp. Sc., Vol. 169, Springer Verlag, 1984.
21. T. Helleseeth, "Some Results about The Cross-Correlation Function Between Two Maximal Linear Sequences", Discrete Mathematics, 16, 1976, pp 209-232.
22. P. Delsarte, "An Algebraic Approach to the Association Schemes of Coding Theory ", Ph.D thesis, Philips Research reports Suppl. 10(1973).
23. S.W. Golomb, "Correlation Properties of Periodic and Aperiodic Sequences, and Applications to Multi-User Systems", in Proceedings of the NATO Study Institute on New Concepts in Multi-User Communication, Norwich, UK, J.K. Skwirzynski, Ed., 1982.
24. F.J. MacWilliams and N.J.A Sloane, "The Theory of Error-Correcting Codes", north-holland, 1981.
25. H. Bhat, "Linear Sequential Systems over Residue Class Polynomial Rings: Theory and Applications", Ph.D. Thesis, Department of Electrical Engineering, I.I.T, Kanpur, 1985.
26. Y. Nishikado, M. Sato, M. kasahara, T. Mamakewa and K. Harada, "A New Encoding and Decoding Schemes for Multiple Access Channels", Electronics and Communication in Japan, Vol. 61-A, No. 4, 1978, pp 37-44.
27. J.L. Massey, "A Short Introduction To Coding Theory and Practice", Proceedings, International Symposium on Signals Systems and Electronics (ISSSE'89), Erlangen, Germany, Sept. 1989, pp 629-633.
28. H.-A. Loeliger, "Signal Sets Matched To Groups", IEEE Trans. Inform. Theory, IT-37, No. 6, Nov. 1991, pp 1675-1682.
29. P. Udaya, M.U. Siddiqi, "Optimal Quadriphase Sequences Derived from Maximal Length Sequences", Submitted to Journal of Applicable Algebra in Engineering, Communication and Computing, Springer-Verlag.
30. P. Udaya and M.U. Siddiqi, "Large Linear Complexity Sequences over  $Z_4$  for Quadriphase Modulated communication Systems having Large Linear Complexity", pp 386, Proceedings, 1991 IEEE International Symposium on Information Theory, Budapest June 24-28, 1991.
31. P. Sole, "A Quarternary Cyclic Code, and a Family of Quadriphase Sequences with Low Correlation Properties", Coding theory and applications, Lecture notes in Comp. Sc., Vol. 388. 1989.
32. S. Boztas and P. V. Kumar, "Near-Optimal Sequences for CDMA", Proceedings 1991 IEEE International Symposium on Information Theory, Budapest, June 24-28, 1991. pp 282.
33. S. Boztas, Hammons, and P. V. Kumar, "Near-Optimal Sequences for CDMA", IEEE Trans Inform. Theory, Vol. IT-38, No. 3, May 1992, pp 1101-1113.
34. L.R. Welch, "Lower Bounds on the Maximum Cross Correlation on the Signals", IEEE Trans. Inform. Theory, IT-24, Sep 1978, pp 537-545.
35. V.M. Sidel'nikov, "On Mutual Correlation of Sequences", Soviet Math. Dokl., Vol. 12, No. 1, 1971, pp 197-201.
36. W.S. Jibrail and A.R.J. Houmadi, "Acquisition of Direct Sequence Spread Spectrum Signals using Sliding Correlators", Int. J. Electronics, Vol. 71, No. 5, 1991, pp 733-743.

37. D.A. Bollman, "Some Periodicity Properties of Transformations On Vector Spaces Over Residue Class Rings", J. Soc. Indust. Appl. Math., Vol. 13, No. 3, Sept 1965, pp 902-912.
38. D.A. Bollman, "Some Periodicity Properties of Modules Over The Ring of Polynomials with Coefficients in a Residue Class Ring", J. SIAM Appl. Math., Vol. 14, No. 2, March 1966, pp 237-241.
39. B. Sundar Rajan "Transform Domain Study of Cyclic and Abelian Codes over Residue Class Integer Rings", Ph.D. Thesis, Department of Electrical Engineering, I.I.T, Kanpur, 1989.
40. R.A. Liebler and R.A. Mena, "Certain Distance-Regular Digraphs and related rings of Characteristic 4" J. Combin. Theory, Series A 47, 1988, pp 111-123.
41. J.L. Massey, "On Welch's Bound for the Correlation of a Sequence Set", IEEE Int. Symp. Inform. Theory, Budapest, Hungary, June 24-28, 1991, pp 385.
42. A.A. Shaar and P.A. Davies, "A Survey of One-coincidence Sequences for Frequency-hopped Spread-spectrum Systems", IEE Proceedings, Vol. 131, Pt F, No. 7, Dec. 1984, pp 719-724.
43. J. J. Komo and S. C. Liu, "Maximal Length Sequences for Frequency Hopping", IEEE Journal on Selected Areas in Communications, Vol. 8, No. 5, June 1990, pp 819-822.
44. J.L. Massey, "Shift Register Synthesis and BCH Decoding", IEEE Trans. Inform. Theory, IT-15, 1969, pp 122-127.
45. J.A. Reeds and N.J.A. Sloane, "Shift Register Synthesis (modulo m)", SIAM J. Comp., Vol. 14, No. 3, 1985.
46. J.L. Massey and T. Schaub, "Linear Complexity in Coding Theory", Coding Theory and Applications, Lecture Notes in Comp. Sc. Vol. 311. 1988
47. T. Siegenthaler and R. Forre, "Generation of Binary Sequences with Controllable Complexity and Ideal r-tuple Distribution", EUROCRYPT-85, Lecture Notes in Comp. Sc., Vol. 219, 1985.
48. R.A. Scholtz and L.R. Welch, "GMW Sequences", IEEE Trans. Inform. Theory, IT-30, May 1984, pp 548-553.
49. L.D. Baumert, "Cyclic Difference Sets", Lecture Notes in Mathematics, Vol. 182, New York: Springer Verlag, 1971
50. E.C. Posner, "Combinatorial Structure in Planetary Reconnaissance", in Error Correcting Codes, H.B. Mann, Ed., New York: Wiley, 1969, pp 15-46.
51. B. Gordon, W.H. Mills and L.R. Welch, "Some New Difference Sets", Canadian J. Math., Vol. 14, 1962, pp 614-625
52. J. Lindner, "Binary Sequence Up to Length 40 with Best Possible Autocorrelation Function", Electronics Letters, Vol. 11, No. 21, 16<sup>th</sup> October 1975, pp 507.
53. U. Somaini, "Binary Sequences with Good Correlation Properties", Vol. 11, No. 13, 26<sup>th</sup> June 1975, pp 278-279.
54. N. Zierler, "Linear Recurring Sequences", J. SIAM, Vol. 7, March 1959, pp 31-48.
55. M. Hall, "An Isomorphism between Linear Recurring Sequences and Algebraic Rings", Trans. Amer. Math. Soc., Vol. 43, May 1938, pp 377-385

56. M. Ward, "The Arithmetical Theory of Linear Recurring Sequences", Trans. Amer. Math. Soc, Vol. 35, July 1933, pp 600-628.
57. D.A Huffman, "The Generation of Impulse-equivalent Pulse Trains", IRE Trans. Inform. Theory, Vol. IT-8, 1962, pp s10-s16.
58. R. Gold, "Maximal Recursive Sequences with 3-Valued Recursive Cross-Correlation Functions", IEEE Trans. Inform. Theory, IT-14, Jan 1968 pp 154-156.
59. R. Gold, "Optimal Binary Sequences for Spread Spectrum Multiplexing", IEEE Trans. Inform. Theory, IT-13, Oct. 1967 pp 616-621.
60. T. Kasami, "Weight Distribution of Bose-Choudhury-Hocquenghem Codes", in Key Papers in the Development of Coding Theory, E.R. Berlekamp, Ed. New York: IEEE Press, 1974.
61. J.D. Olsen, R.A. Scholtz, and L.R. Welch, "Bent-function Sequences", IEEE Trans. Inform. Theory, IT-28, Nov. 1982, pp 858-864.
62. J.S. No and P.V. Kumar, "A New Family of Binary Pseudorandom Sequences Having Optimal Periodic Correlation Properties and Large Linear Span", IEEE Trans. Inform. Theory, IT-35, March 1989, pp 371-379.
63. P.V. Kumar and O. Moreno, "Polyphase Sequences with Periodic Correlation Properties better than Binary Sequences", IEEE Trans. Inform. Theory, IT-37, May 1991, pp 603-616.
64. S. Chang Liu and J.J. Komo, "Nonbinary Kasami Sequences over  $GF(p)$ ", Proceedings, 1991 IEEE International Symposium on Information Theory, Budapest June 24-28, 1991.
65. T. Moriuchi and K. Imamura, "Balanced Polyphase Sequences with Good Periodic Correlation Properties Obtained from Modified Kumar-Moreno Sequences", 1991 IEEE International Symposium on Information Theory, Budapest June 24-28, 1991.
66. A. Klapper, A.H. Chan and M. Goresky, "Cascaded GMW sequences", Proceedings, 1991 IEEE International Symposium on Information Theory, Budapest June 24-28, 1991.
67. R. Lidl and H. Niederreiter, "Finite Fields" in Encyclopedia of Mathematics and its Applications. Vol.20 Cambridge University Press, 1984.
68. R.E. Blahut, "Theory and Practice of Error Control Codes", Reading, MA: Addison-Wesley, Publishing Company, California, 1983.
69. R.A. Scholtz and L.R. Welch, "Group Characters: Sequences with Good Correlation Properties", IEEE Trans. Inform. Theory, IT-24, Sep. 1978, pp 537-545.
70. P.V. Kumar and C.M. Liu, "On Lower Bounds to the Maximum Correlation of Complex Roots of Unity Sequences", IEEE Trans. Inform. Theory, IT-36, May 1990, pp 633-640.
71. J.E Stalder and C.R. Cahn, "Bounds for Correlation Peaks of Periodic Digital Sequences", Proceedings of the IEEE, Vol. 52, Oct. 1964, pp 1262-1263
72. P. Piret, "Bounds for Codes Over the Unit Circle", IEEE Trans. Inform. Theory, IT-32, No. 6, Nov 1986, pp 760-767.
73. S.W. Golomb and H. Taylor, "Construction and Properties of Costas Arrays", Proceedings of the IEEE, Vol. 72, No. 9, Sept. 1984, pp 1143-1153.
74. B.M. Popovic, "Comments on "Code Acquisition for a Frequency Hopping System", IEEE Trans. Commun., Vol. 37, No. 5, May 1989, pp 540-541.

75. B.M. Popovic, "New Sequences for asynchronous Frequency Hopping Multiplex", *Electrn. Lett.*, Vol. 22, No. 12, June 5, 1986, pp 640–642.
76. P.V. Kumar, "Frequency–Hopping Code Sequence Designs Having Large Linear Span", *IEEE Trans. Inform. Theory*, IT–34, No. 1, Jan 1988, pp 146–151.
77. J.J. Komo, "Crosscorrelation of  $m$ –sequences over Non–prime Fields", *Electronics Letters*, Vol. 24, No. 4, 1989, pp 288–289.
78. W.J. Park and J.J Komo, "The Autocorrelations of  $m$ –sequences over non–prime Finite Fields", *IEEE Trans, AES* 24, 1988, pp 459–461.
79. W.J. Park and J.J Komo, " Relationship between  $m$ –sequences over  $GF(q)$  and  $GF(q^m)$ ", *IEEE Trans. Inform. Theory*, IT–35, Jan 1989, pp 183–186.
80. J. Chung–yaw Chang and J.K. Wolf, "On Channels and Codes for the Lee Metric", *Information and Control* 19, 1971, pp 159–173.
81. E.J. Groth, "Generation of Binary Sequences With Controllable Complexity", *IEEE Trans. Inform. Theory*, Vol. IT–17, No. 3 May 1971, pp 288–296.
82. E.L. Key, "An Analysis of the Structure and Complexity of Nonlinear Binary Sequence Generators", *IEEE Trans. Inform. Theory*, Vol. IT–22, No. 6 November 1976, pp 732–736.
83. L. Brynielson, "On the Linear Complexity of Combined Shift Register Sequences.,EUROCRYPT–85, Lecture Notes in Comp. Sc. Vol. 219. 1985.
84. A.H. Chan, M. Goresky and A. Klapper, "Correlation functions of Geometric Sequences", *Eurocrypt–90, Lecture Notes in Comp. Sc.*, Vol. 473, Springer Verlag, pp 214–221.
85. Z. Dai, T. Beth, and D. Gollmann, "Lower bounds for the Linear Complexity of Sequences over Residue rings", *Eurocrypt–90, Lect. Notes in Comp. Sc.*, Vol. 473, Springer Verlag, pp 189–195.
86. H. Murakami, I.S. Reed and L.R Welch, "A Transform Decoder for Reed–Solomon Codes in Multiple User Communication Systems", *IEEE Trans. Inform. Theory*, IT–23, 1977, pp 1745–1753.
87. R. Raghavendran, "Finite Associative Rings", *COMPOSITIO MATHEMATICA*, Vol. 21, Fasc. 2, 1969, pp 195–220.
88. B.R. Mc Donald , "Finite Rings with Identity", New York: Marcel Dekker, 1974.
89. E. Bannai and T. Ito, "Algebraic Combinatorics I, Association Schemes", California: The Benjamin/Cummings Publ. Comp, 1984.
90. J.M. Goethals, "Association Schemes", In *Algebraic Coding Theory and Applications*, G. Longo and P. Heartmann, Eds.
91. I. Niven and H.S. Zuckerman, "An Introduction to the Theory of Numbers", Wiley Eastern, 1976.
92. A.J. Kempner, "Polynomials and their Residue Systems", *Trans. Amer. Math. Soc.*, Vol. 22, 1921, pp 240–266, 267–288.
93. B. Sklar, "Digital Communications", Chapter 10, Prentice–Hall, Englewood Cliffs, 1988.
94. I.N. Herstein, "Topics in Algebra", John Wiley, 1984.
95. H.L. Clasen, "Studies of the Multiplications in  $GF(q)[x]/(a(x))$ ", Ph.D Thesis, Department of Mathematics and Informatics, Delft University of Technology, Netherlands. 1978.